



App Layering

Machine translated content

Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

Contents

Novedades	5
Elementos retirados	30
Problemas conocidos	31
Requisitos del sistema	41
Planificar su implementación	45
XenServer	57
Citrix Provisioning	58
Docker	60
Cloud de Google	61
Machine Creation for Azure o Azure Government	62
Creación de máquinas para XenServer	63
Creación de máquinas para Google Cloud	64
Machine Creation for Hyper-V	65
Machine Creation for Nutanix AHV	65
Machine Creation for vSphere	67
MS Azure o Azure Government	70
MS Hyper-V	71
Nutanix AHV	73
VMware vSphere	74
Recursos compartidos de archivos de red (otras plataformas)	76
Instalar el dispositivo	76
XenServer	77
Cloud de Google	79

MS Azure o Azure Government	88
MS Hyper-V	91
Nutanix AHV	94
VMware vSphere	97
Instalar el agente de App Layering	103
Configurar	107
Consola de administración de acceso	107
Cambiar contraseñas de administrador	108
Configurar el recurso compartido de archivos	109
Conectarse a un servicio de directorios	111
Asignar roles	113
Actualizaciones	115
Configuraciones de conectores	121
Implementaciones de Azure	128
Creación de plantillas ARM	134
Plantillas de inicio	144
Parámetros de plantilla	173
XenServer	182
Citrix Provisioning (XenServer, VMware, Hyper-V, Nutanix)	187
Cloud de Google	192
Machine Creation for Azure	195
Machine Creation for Azure Government	197
Creación de máquinas para XenServer	199
Machine Creation for Hyper-V	204

Creación de máquinas para Google Cloud	207
Creación de máquinas para Nutanix AHV (Acropolis)	210
Machine Creation for vSphere	214
MS Azure	220
MS Azure Government	227
MS Hyper-V	235
Nutanix AHV (Acropolis)	239
VMware vSphere	243
Recursos compartidos de archivos de red	251
Uso compartido de archivos de Windows	252
Capa	254
Preparar el sistema operativo para la distribución por capas	259
Preparar la imagen del sistema operativo para la disposición en capas en XenServer, Hyper-V o vSphere	262
Preparar la imagen del sistema operativo para la colocación en capas en Google Cloud	268
Preparar la imagen del sistema operativo para la disposición en capas en Azure	271
Preparar la imagen del sistema operativo para la disposición en capas en Nutanix	276
Crear la capa de SO	282
Crear capa de plataforma	284
Crear o clonar una capa de aplicación	296
Aplicaciones antivirus de las capas	307
Instrucciones sobre App Layering	308
Implementar capas de aplicaciones como capas elásticas	309
Implementar capas de usuarios	320

Actualizar capa	343
Exportar e importar capas	348
Excluir archivos de capas (función avanzada)	353
Publicar	356
Crear o clonar una plantilla de imagen	356
Publicar imágenes en capas desde una plantilla	359
Administrar una plantilla de imagen	361
Administrar	363
Configuración del sistema	363
Almacenamiento	367
Configuración del dispositivo	371
Servicios App Layering	373
Servicio de directorios	375
Usuarios	378
Grupos y usuarios	378
Puertos de firewall	379

Novedades

June 27, 2024

Citrix ofrece nuevas funciones y mejoras a los usuarios de Citrix App Layering cuando están disponibles. Las nuevas versiones agregan valor al producto y no hay motivo para retrasar el momento de actualizar.

Este artículo cubre las funciones nuevas y mejoradas, junto con los problemas resueltos en esta versión.

Para conocer los requisitos de App Layering más recientes y las plataformas compatibles, consulta [Requisitos del sistema](#).

App Layering 2403 (esta versión)

Esta versión contiene las siguientes funciones nuevas:

- **Citrix Hypervisor cambió su nombre a XenServer**

De acuerdo con nuestra última estrategia de cambio de marca, hemos actualizado todas las instancias de Citrix Hypervisor a XenServer.

- **Actualización de Herramientas de máquina de SO**

Las herramientas de máquina del sistema operativo ahora están actualizadas para incluir la limpieza automática de las carpetas INF vacías que pueden provocar errores en la reconstrucción del contador de rendimiento. Debe crear una nueva revisión de la capa de su sistema operativo y aplicar las herramientas de máquina del sistema operativo a la capa.

Nota: No lo ejecute `setup_x64.exe` en una revisión del sistema operativo. La aplicación solo es necesaria antes de importar un sistema operativo en ELM, y ejecutarla en una revisión del sistema operativo puede provocar problemas desconocidos.

- **Las tareas de creación de capas muestran más información sobre la máquina de empaquetado**

El estado de acción requerida de las tareas de creación de capas ahora incluye otra información sobre la máquina de empaquetado, aparte del nombre de la máquina virtual cuando se utiliza la composición de descarga. Para la mayoría de los tipos de conectores, la información adicional es la dirección IP de la máquina.

- Para los tipos de conectores AHV de Nutanix, se muestra un enlace a la máquina de empaquetado en la interfaz de usuario de Nutanix Prism.

- Los tipos de conectores de implementación de Azure permiten proporcionar información personalizada a través de las plantillas ARM. Para obtener más información, consulte [Salida de la máquina](#).
- **Nuevo conector: recurso compartido de archivos de Windows**

La interfaz de usuario de **Connectors** ahora incluye **Windows File Share**. Este conector permite al usuario publicar un disco en un recurso compartido de archivos, aprovechando una configuración de conectores existente con descarga habilitada.

Para obtener más información, consulte [Uso compartido de archivos de Windows](#).

- **Capa de personalización de usuarios: Recuperación de espacio de capa de usuarios/UPL**

Anteriormente, Windows utilizaba primero los bloques no utilizados de un disco, lo que requería una gran cantidad de espacio en el servidor de archivos de back-end. Al utilizar el nuevo proceso de recuperación de espacio VHDX, los archivos VHDX de la capa de usuario se optimizan automáticamente cada vez que el usuario cierra sesión.

Para obtener más información, consulte [Recuperación de espacio de capa de usuarios/UPL](#).

Correcciones

- Las aplicaciones AppV integradas no funcionan con las imágenes compatibles con PVS EL. [ALHELP-1717]
- La publicación del conector PVS falla si la ruta del recurso compartido tiene una barra invertida al final. [UNI-89881]
- Al crear una capa de sistema operativo a partir de una máquina virtual Gold de XenServer con cadenas de BIOS personalizadas, el script `ImportOsLayer.ps1` no determina el tipo de hipervisor y produce el siguiente error:
`Offload Compositing is not supported on this hypervisor yet`
El tipo de hipervisor ahora se puede especificar explícitamente mediante el parámetro `-HypervisorType` para evitar este problema. [UNI-90521]

App Layering 2312

Esta versión contiene las siguientes funciones nuevas:

- **Conector Nutanix AHV nuevo y mejorado.** Al crear y administrar el conector AHV de Nutanix en App Layering, ahora puede disfrutar de la nueva interfaz de usuario con el soporte de hipervisor modernizado. Para obtener más información, consulte [Conector AHV de Nutanix](#). Esta versión también presenta la compatibilidad con la **composición** de descarga para capas y plantillas

de imágenes en Nutanix AHV. Las tecnologías de virtualización modernas, como UEFI, vTPM y Secure Boot, ahora están disponibles con **Composición de descarga**. Para obtener más información, consulte [Acerca de la composición de descargas](#).

- **Nuevo enfoque para anular la exclusión** de archivos . Ahora puede anular las exclusiones de archivos actualizando la herramienta Gold Image para introducir y acumular exclusiones predefinidas para el sistema de archivos de App Layer. Para obtener más información, consulta [Exclusiones](#) predefinidas .

Correcciones

- Los valores o subclaves de las claves `HKLM\Software\Wow6432Node\Citrix\PortICA\Policy\Session\PolicyInputValues` y `HKLM\SOFTWARE\Citrix\VirtualDesktopAgent\Policy\Session\PolicyInputValues` no persisten entre los inicios de sesión. [UNI-89899]
- Cuando publicas una imagen con la versión 2306 de App Layering, no puedes ver las nuevas herramientas de imagen, como AppRulesCompare, en la imagen. [UNI-89936]
- Se puede producir un error de inicio o cierre de sesión cuando FSLogix usa ubicaciones de Cloud Cache para contenedores de perfiles o ODFC junto con App Layering Elastic Layers. Una pantalla emergente muestra los errores de inicio de sesión y una pantalla de cierre de sesión inmovilizada muestra los errores de cierre de sesión. Los archivos de registro de FSLogix ubicados en `c:/ProgramData/FSLogix/Logs/Profile/Profile-YYYYMMDD.log` también muestran el siguiente mensaje de error en caso de errores de inicio de sesión: `"ERROR:00000005 Access is denied"` errors at various points during the login attempt.

App Layering 2309

Esta versión contiene las siguientes funciones nuevas:

- **Opción para mantener la máquina de implementación de MCS en funcionamiento.** Si desea personalizar las imágenes implementadas desde el ELM cuando la máquina arrancada se prepara para su implementación en MCS, debe actualizar las herramientas de la máquina en la revisión del sistema operativo a la revisión 2309 o posterior. Para obtener más información, consulte [Crear capa de plataforma](#).
- **Compatibilidad con el formato VHDX para capas de usuarios.** Las capas de usuarios ahora se crean con el formato VHDX en lugar del formato VHD, como en las versiones anteriores. No es necesario convertir las capas de usuarios existentes con el formato VHD a VHDX. Sin embargo, si desea convertir las capas de usuario manualmente, se utilizará el formato VHDX

de la capa si ambas siguen en la misma carpeta. Si desea crear nuevas capas de usuarios con el formato VHD, puede desactivar la función. Para obtener más información, consulte [Habilitar la capa de usuarios](#).

- **La opción de cambio de capa de sistema operativo para capas elásticas ahora está habilitada de forma predeterminada en la interfaz de usuario de App Layering.** Ya no tiene que habilitar manualmente la nueva opción de cambio de capa del sistema operativo. Para obtener más información, consulte [Cambio de capa de sistema operativo para capas elásticas](#).
- **Nueva opción de plantilla de imagen: desfragmente el disco al publicar la plantilla de imagen.** Ahora puede usar la nueva opción de plantilla de imagen que optimiza la imagen publicada creada desde el dispositivo App Layering. Esta opción solo está disponible cuando se selecciona un conector de composición de descarga. Para obtener más información, consulte [Crear una plantilla de imagen desde cero](#).
- **Citrix Hypervisor nuevo y mejorado.** Al crear y administrar el conector de Citrix Hypervisor en App Layering, ahora puede disfrutar de la nueva interfaz de usuario con la compatibilidad modernizada con Hypervisor. Para obtener más información, consulte [Citrix Hypervisor](#). Esta versión también presenta la compatibilidad con la composición de descarga para capas y plantillas de imágenes en Citrix Hypervisor. Las tecnologías de virtualización modernas, como UEFI, vTPM y Secure Boot, ahora están disponibles con Composición de descarga. Para obtener más información, consulte [Acerca de la composición de descargas](#).

Correcciones

- Hay una pérdida de memoria en las imágenes que tienen habilitada la estratificación elástica y Sentinel One instalado. [ALHELP-1708]
- La publicación de imágenes con muchas capas puede fallar debido a las limitaciones de tamaño de la base de datos.
- El proceso LSASS se bloquea en algunos archivos y provoca un error en el proceso de arranque. [ALHELP-1710]
- VMware vSphere falla con tipos de objetos no válidos.
- Las esperas del modo de error de purga están causando problemas de rendimiento. [UNI-89518]
- Los hosts de sesión se bloquean la primera vez que se inicia sesión. [ALHELP-1722]
- Es posible que los paquetes de AppV, cuando están preinstalados en una capa de aplicación, no se inicien o se inicien, pero no funcionen correctamente. [ALHELP-1717]

App Layering 2306

Esta versión contiene las siguientes funciones nuevas:

- **El control de acceso basado en roles ahora está disponible en la nueva interfaz de usuario de App Layering.** Ahora puede asignar roles a los usuarios de App Layering, definiendo a qué funciones pueden acceder. Cualquier usuario al que se le asigne un rol puede iniciar sesión en la consola de administración. Para obtener más información, consulte [Asignar roles](#).
- **Se retiró la compatibilidad con Windows 7 y 32 bits del ELM.** Todas las capas del sistema operativo Windows de 7 y 32 bits se han descontinuado y no son compatibles con varias versiones del ELM. Si todavía utiliza un sistema operativo Windows de 7 o 32 bits no compatible, no lo actualice a esta nueva versión sin antes hacer una copia de reserva de su ELM y, a continuación, haber contactado con el equipo de asistencia para conocer las opciones.
- **Nueva herramienta de App Layering: ScanWritableFiles.** ScanWritableFiles es una aplicación en la que los usuarios pueden identificar archivos y carpetas que solo existen en la capa en la que se puede escribir (como la capa de usuario). Por lo tanto, estos objetos del sistema de archivos no se encuentran en ninguna otra capa o volumen, como la imagen base o cualquier capa asignada elásticamente. La identificación de los objetos del sistema de archivos de este tipo puede resultar útil cuando:
 - Determinar qué objetos se pueden eliminar de forma segura sin afectar a las aplicaciones asignadas elásticamente
 - Identificar los componentes de la aplicación instalados directamente por el usuario, en lugar de proporcionarlos la imagen o cualquier capa elástica
 - Identificación de los componentes de la aplicación instalados en una máquina de empaquetado

Para obtener más información detallada, consulte [C:\Program Files\Unidesk\Tools\ScanWritableFiles\ReadMe.txt](#).

- **Nueva herramienta de App Layering: AppRuleCompare.** AppRuleCompare analiza los posibles conflictos del sistema de archivos y el registro entre las capas de aplicaciones, incluida la capa de plataforma, si está presente. Cuando se ejecuta directamente en una máquina con capas de aplicaciones, AppRuleCompare “procesa” los archivos AppRule asociados a las capas integradas en la imagen base, así como los que se han unido elásticamente a la máquina. Para obtener más información detallada, consulte [C:\Program Files\Unidesk\Tools\AppRuleCompare\ReadMe.txt](#).

Correcciones

- En algunos servidores de Provisioning, el comando para montar un recurso compartido de archivos con un agente de App Layering posterior a la versión 2003 se bloquea indefinidamente. [ALHELP-1593]
- Cuando se crea o se cambia el nombre de un archivo o directorio, CFS también cambia el nombre abreviado del objeto, lo que provoca notificaciones de directorio inesperadas. [ALHELP-1682]
- Un error en la rutina generatePerfGenRecompileScript está provocando un error en el BIC. [UNI-89255]
- La operación de cambio de nombre está fallando debido a un error en nuestra lógica de cambio de nombre. [UNI-89256]
- Se produce un error de firma digital del controlador en 2012R2 después de cambiar a una nueva certificación de Citrix. [UNI-89258]
- La nueva interfaz de usuario del conector de vSphere no incluye todos los hosts. [UNI-89314]
- El VDS no detecta un disco virtual recién conectado. [ALHELP-1694]

App Layering 2304

Esta versión contiene las siguientes funciones nuevas:

- **Soporte de credenciales de registro para implementaciones de Azure.** Ahora puede usar las credenciales de registro para configurar el conector de Azure Deployments, de forma similar a lo que estaba disponible para el conector de Azure heredado. Para obtener más información, consulte [Azure Deployments](#).
- **Ahora puede definir rutas de directorio que no se redirijan a la capa de usuarios con la directiva de exclusiones de usuarios de Citrix Studio.** Algunas cosas a tener en cuenta:
 - Las exclusiones de usuarios no anulan AlwaysOnBoot.
 - Las exclusiones de usuarios se aplican a toda la capa de usuarios y a la capa de personalización de usuarios (UPL), pero no al anfitrión de la sesión. El anfitrión de la sesión ignora las exclusiones de usuarios y agrega el mensaje a la capa de usuarios.
 - Logoff.txt ahora contiene todas las exclusiones de usuarios activas.
- **Compatibilidad con atributos personalizados de Active Directory (AD).** Ahora puede usar atributos de AD personalizados en una ruta de capa de usuario para las capas de usuarios y las capas de personalización de usuarios (UPL). Los atributos de AD deben incluirse en hashes (por ejemplo, #sAMAccountName#). Para obtener más información, consulte [Implementar capas de usuarios](#) y [Capa de personalización de usuarios](#).

- **Nueva interfaz de usuario para el conector VMware vSphere.** El conector VMware vSphere ahora tiene una nueva interfaz de usuario. Para obtener más información, consulte [VMware vSphere](#).
- **Los contadores de rendimiento ahora funcionan desde cualquier capa, incluidas las capas de aplicaciones y las capas de usuarios completos.** Las herramientas de imagen doradas deben actualizarse en la revisión del sistema operativo para garantizar que los contadores de rendimiento se reconstruyan correctamente al arrancar una imagen. La revisión del sistema operativo necesita al menos una reconstrucción de los contadores de rendimiento. Abra una ventana de comandos de administrador en la misma revisión del sistema operativo en la que está actualizando la imagen dorada y ejecute los comandos `c:\windows\system32\lodctr /ryc:\windows\syswow64\lodctr \r`.
- **MSMQ ahora se puede usar desde cualquier capa incluida en la imagen.** Las herramientas de imagen doradas deben actualizarse en la revisión del sistema operativo para garantizar que MSMQ se haya restablecido e iniciado correctamente, cuando esté presente. Hay un nuevo archivo de registro denominado `GenRandomQMID.log` para indicar las acciones de `C:\Windows\setup\scripts\kmsdir\GenRandomQMID.ps1`. Esto permite que MSMQ se inicie correctamente independientemente de dónde se haya instalado.

Correcciones

- La falta de una clave de perfil provoca un error en el montaje de la capa de usuario. [UNI-88890]
- Código de notificación de directorio que provoca picos de uso de la CPU al desconectar una capa elástica de una máquina en ejecución. [ALHELP-1614]
- La herramienta `generate.pl` configuró la clave `HKLM\System\WPA` de **Nunca virtualizar a Virtualizar siempre**, lo que provocó la pérdida de la clave de activación de Windows. [ALHELP-1673]
- FSLogix que se ejecutaba con una capa de usuarios completa no pudo iniciar sesión en el tercer inicio de sesión y en los siguientes, lo que provocó perfiles duplicados y otros problemas. [ALHELP-1672]
- Al eliminar y volver a crear las claves volátiles, los controladores de consultas impidan que la persona que llama vea la imagen. [ALHELP-1648]
- Los sondeos de archivos de SessionHost faltan algunos archivos, lo que provoca conflictos y hace que las capas no funcionen. [ALHELP-1653]
- Se mejoró el rendimiento de los tiempos de enumeración en dirección inversa. [ALHELP-1642]
- La lógica de escaneo del contador de rendimiento abre los archivos en el modo de solo lectura o uso compartido y no se puede desactivar, lo que provoca algunos conflictos con los archivos

que el entorno del usuario debe actualizar continuamente. La lógica de análisis del contador de rendimiento ahora abre los archivos en el modo de lectura y uso compartido no denegado y se puede desactivar si es necesario. [ALHELP-1679]

- La itinerancia de búsqueda de FSLogix a veces no funciona correctamente en imágenes exclusivas de Elastic Layer debido a una nueva función, que se invoca antes del inicio de sesión del usuario antes de que se virtualicen las colmenas de capas. [ALHELP-1669]
- La función MSMQ de Microsoft no funciona al finalizar la imagen. [ALHELP-1641]

App Layering 2211

Esta versión contiene las siguientes funciones nuevas:

- **Nuevos conectores de Azure Deployments.** Se han creado e implementado dos nuevos conectores de Azure en App Layering: Azure Deployments y Machine Creation for Azure Deployments. Ambos conectores también son compatibles con entornos gubernamentales (Azure Government y Machine Creation for Azure Government, respectivamente). El antiguo conector de Azure y el conector de creación de máquinas para Azure (así como sus homólogos gubernamentales) ya están en desuso, pero siguen disponibles para su uso durante un tiempo limitado. Para obtener más información, consulte [Implementaciones de Azure](#).
- **La capa de plataforma de bloques finaliza si se detecta una clave RSA WEM.** Si la clave RSA de WEM existe en la capa de plataforma, se deben a problemas con Workspace Environment Management (WEM). Si se detecta la clave RSA, ahora recibirá un mensaje antes de finalizar la capa de plataforma para eliminar la clave. Consulte [Crear capa de plataforma](#) para obtener más información.
- **Se ha mejorado el mecanismo de falta de caché.** El valor predeterminado para las entradas del mecanismo de falta de caché se ha incrementado de 256 entradas a 1024 entradas. Si ha aumentado el tamaño predeterminado mediante una configuración del registro, debe eliminar la configuración personalizada para que esta mejora funcione correctamente.
- **Los controladores de fabricantes de equipo original persisten en la capa de usuarios.** Ahora, los controladores de fabricantes de equipo original (como los controladores de impresora) se pueden almacenar en la capa de usuarios y no es necesario instalarlos de nuevo después de cada inicio de sesión del usuario. Los posibles conflictos de nombres entre los controladores de fabricantes de equipo original entre la imagen del sistema operativo y la capa de usuarios se resuelven automáticamente. Tras actualizar la versión, las capas de usuarios existentes se escanean para detectar cualquier rastro de fabricantes de equipo original inesperado.
- **Compatibilidad con Windows 10 y 11 22H2.** Ahora puede usar Windows 10 y 11 22H2 como sistema operativo para imágenes en capas. Para obtener más información, consulte [Requisitos](#)

del sistema.

Correcciones

- Se ha corregido un problema que se producía al agregar el archivo GAC_MSIL a la lista AOB del Registro. Se ha eliminado el archivo GAC_MSIL. [ALHELP-1612]
- Se agregó una nueva configuración de ulayer (HKLM\Software\Unidesk\ULayer\BasicAADScrubEnabled [dword]) que permite inhabilitar la eliminación por parte de Azure del registro y las ubicaciones de archivos de Windows 10. De forma predeterminada, esta configuración se establece en true. [UNI-87854]
- Se ha corregido un error que provocaba que las demoras en el modo de purga hicieran que los archivos se abrieran solo para lectura, lo que provocaba que el sistema funcionara lentamente. [ALHELP-1621]
- Se ha corregido un error que provocaba que las claves de `C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys` se quitaran al finalizar. El BIC ahora incluye esta carpeta. [ALHELP-1623]
- Se ha corregido un problema por el que se eliminaban algunas directivas locales tras una actualización del sistema operativo Machine Tools. El gposetup.cmd estaba realizando una inicialización adicional y sobrescribiendo el archivo gpt.ini por el archivo defaultgpt.ini. [ALHELP-1627]
- Se ha corregido un problema que provocaba que las listas de control de acceso se ordenaran incorrectamente en las carpetas recién creadas. El problema provocó que algunas entradas de estas carpetas no fueran efectivas. [ALHELP-1632]

App Layering 2208

Esta versión contiene las siguientes funciones nuevas:

- **Ahora se permite que los caracteres comodín excluyan un directorio de una capa compuesta.** Solo se puede usar un directorio como comodín y solo un * se puede usar en una sola ruta. Consulte [Excluir archivos de las capas](#) para obtener más información.

Correcciones

- La selección de capas para la exportación ya no deja de guardarse después de actualizar a la versión 2206. [ALHELP-1605]

- Se han corregido problemas con ciertas aplicaciones que se producían tras actualizar a la 2206. El directorio `C:\Windows\Microsoft.NET\assembly\GAC_MSIL` ya no se excluye de las capas de aplicaciones y el directorio `c:\windows\system32\wbem\repository` solo se permite en la capa de plataforma. [UNI-87356]

App Layering 2206

Esta versión contiene las siguientes funciones nuevas:

- **Se ha eliminado Microsoft Silverlight.** App Layering ya no requiere ni admite MS Silverlight. Consulte [Requisitos del sistema](#) para obtener más información.
- **Se han movido algunos elementos del menú de la ficha Usuario a la ficha Sistema en la nueva interfaz de usuario:**
 - Administración del acceso a roles para usuarios y grupos de Active Directory
 - Crear, eliminar y modificar cruces de directorios en el servicio de directorios
- **Se han convertido más funciones de administración en la nueva interfaz de usuario.** Las siguientes funciones ya están disponibles en la nueva interfaz:
 - Importación y exportación de capas
 - **Sistema:** Ubicaciones de almacenamiento de capa de usuarios
- **¡Nueva interfaz de usuario completamente implementada!** Con la finalización de lo anterior, la nueva interfaz de usuario se implementa por completo, y ahora toda la documentación lo refleja. Muchos procedimientos y secciones de la documentación se han actualizado con los nuevos flujos de trabajo de blade, sustituyendo los cuadros de diálogo del asistente de la antigua interfaz de usuario.
- **Configuración de firewall personalizada en la capa de usuarios.** Los administradores ahora pueden crear un script que se ejecute automáticamente al iniciar sesión en una capa de usuarios para configurar las opciones y reglas del firewall para un usuario. El script se encuentra `PrivilegedLogon.cmd` y se puede encontrar en `C:\Program Files\Unidesk\Uniservice\UserScripts`.

Correcciones

- NVivo ya no se bloquea cuando se asigna de forma elástica con la capa de usuarios completa habilitada. [ALHELP-1564]
- Ahora se pueden eliminar las carpetas de una imagen publicada tras la actualización. [ALHELP-1582]

App Layering 2204

Esta versión contiene las siguientes funciones nuevas:

- **Compatibilidad con Microsoft Office 2021.** Office 2021 ahora se puede usar con Citrix App Layering.
- **Se han convertido más funciones de administración en la nueva interfaz de usuario.** Puede acceder a la nueva interfaz mediante una URL única en su explorador web. Con la dirección IP del dispositivo, introduzca la siguiente URL: https://<ip_address_of_new_vm>. Las siguientes funciones ya están disponibles en la nueva interfaz:
 - Ficha Sistema: Administrar dispositivo
 - Ficha Sistema: Parámetros y configuración

Correcciones

- La configuración de los atributos de un directorio ya no falla cuando se encuentra en un volumen de solo lectura (capa elástica de aplicaciones). (ALHELP-1500)

App Layering 2202

Esta versión contiene las siguientes funciones nuevas:

- **Ahora puede forzar la eliminación de archivos de clave maestra para las capas de aplicaciones.** Si recibe una advertencia de Elastic Fit para una capa de aplicaciones debido a cambios en el archivo de clave maestra, puede forzar la eliminación de los archivos de clave maestra modificando la configuración del Registro DeleteMasterKeys. Consulte [Implementar capas de aplicaciones como capas elásticas](#) para obtener más información.
- **El conector de VMware Horizon View está en desuso.** Si habilita o usa este conector, tenga en cuenta que ha quedado obsoleto y se eliminará en una versión futura.
- **Se han convertido más funciones de administración en la nueva interfaz de usuario.** Puede acceder a la nueva interfaz mediante una URL única en su explorador web. Con la dirección IP del dispositivo, introduzca la siguiente URL: https://<ip_address_of_new_vm>.
 - Las siguientes funciones ya están disponibles en la nueva interfaz:
 - * Ficha Sistema: conectores
 - * Ficha Sistema: Parámetros y configuración
 - * Menú de usuario: actualización del dispositivo

Correcciones

- La configuración predeterminada de la marca 'ManageOpenForBackup' se ha cambiado de false a true como una solución alternativa para que las ACL se corrompan en C:\windows\syswow64 y C:\windows\system32 al instalar una aplicación. (ALHELP-1327)
- Las ubicaciones de búsqueda que se quitan con el applet Opciones de indización ahora se eliminan correctamente. (ALHELP-1493)
- La configuración de los atributos de un directorio ya no falla cuando se encuentra en un volumen de solo lectura (capa de aplicación elástica). (ALHELP-1500)
- Las conexiones de los VDA en la capa de usuarios de procesos ahora se distribuyen de manera uniforme en los controladores de dominio. (ALHELP-1535)
- La capa de personalización de usuarios ahora se instala correctamente en XenDesktop. (ALHELP-1545)
- La actualización de Enterprise Layer Manager (ELM) de 21.06 a 21.12 ya no falla. (ALHELP-1559)
- Ahora, la sesión del usuario agota el tiempo de espera correctamente en la nueva interfaz de usuario (UNI-85868)

App Layering 2112

Esta versión presenta una nueva experiencia de administración de App Layering y soporte para versiones adicionales de Windows.

- **Compatibilidad con versiones adicionales de Windows:** Puede usar las siguientes versiones de Windows como capa de sistema operativo en App Layering 2112 y posteriores.
 - Windows Server 2022
 - Windows 10 versión 21H2
 - Windows 11, con la siguiente advertencia

Advertencia:

Para admitir Windows 11 como capa de sistema operativo, debe actualizar el dispositivo de App Layering a la versión 2112. Esa versión le proporciona las actualizaciones necesarias para el generador de scripts de Optimizer, el generador de scripts desatendidos, SetKMS y el instalador invitado para establecer el tipo de sistema operativo. Las herramientas de imagen dorada que se utilizan para configurar la imagen dorada deben estar en la versión 2112 o posterior.

- **Nueva experiencia de administración de App Layering.** Esta versión de App Layering presenta la fase 1 de una experiencia de administración nueva y mejorada. La fase 1 de la nueva

interfaz de usuario coexistirá temporalmente junto con la interfaz de usuario existente en el dispositivo de App Layering. Puede acceder a cada uno a través de una URL única y distinta en su explorador web. Tenga en cuenta que aún no hemos trasladado algunas actividades administrativas fuera de las plantillas y capas de imágenes a la nueva interfaz de usuario. Para ello, es necesario seguir utilizando la interfaz original. Al acceder al dispositivo desde un explorador web moderno, como Chrome, Edge o Firefox, aparece la nueva consola de administración. Si usa Internet Explorer para acceder al dispositivo, aparece la consola de administración heredada.

- Mediante la dirección IP del dispositivo, introduzca la siguiente dirección URL en un explorador web compatible:

https://<ip_address_of_new_vm>

- Funciones disponibles en la nueva interfaz de usuario:
 - * Gestión de plantillas
 - * Gestión de capas de aplicaciones, plataformas y sistemas operativos
 - * Gestión de tareas
 - * Inicio de sesión
 - * asignación de usuarios de Elastic
- Compatibilidad con exploradores:
 - * Microsoft Edge
 - * Google Chrome
 - * Mozilla Firefox

Correcciones

- Office 365: Excel puede dejar de responder en las imágenes creadas en la versión 2110 del dispositivo de App Layering. (ALHELP-1537)
- Cuando se usa Zscaler, se informa de un error de controlador cuando se conecta una capa elástica a la máquina virtual. (ALHELP-1528)
- Office 365: las capas de usuarios no se adjuntan al host de la sesión. El problema se produce debido a un bloqueo de archivos en PEUPTemplate.hive (ALHELP-1525)
- App Layering 2107: Los VDA pueden sufrir una excepción irre recuperable y mostrar una pantalla azul de forma aleatoria. (ALHELP-1436)

App Layering 2110

Esta versión es compatible con:

- VMware Cloud en:
 - Azure
 - Amazon Web Services (AWS)
- El conector de Citrix Provisioning ahora le permite especificar una configuración de conector de hipervisor para usar para la **composición de descarga**. Al seleccionar **Descargar composición en una configuración de** conector de Citrix Provisioning, se admite el formato de disco VHDX, el firmware UEFI y el arranque seguro.
- Si Offload Compositing está habilitado en una configuración de conector de Citrix Provisioning, puede agregar una descripción personalizada al disco virtual en el asistente para publicar imagen. Por ejemplo, si publica una plantilla de imagen con un conector de Citrix Provisioning que tiene habilitada la descarga de composición, puede agregar un comentario en el asistente Publicar imagen en capas y el comentario aparecerá como la descripción del disco virtual resultante. Si la descarga de composición no está habilitada o deja el campo Comentario en blanco, la descripción se establece de forma predeterminada en “Imagen en capas”. La longitud máxima de la descripción de un disco virtual es de 250 caracteres. Si es más largo, se trunca.
- (Función avanzada) Ahora puede excluir archivos y carpetas específicos de una capa compuesta para evitar que los archivos persistan en el escritorio del usuario. Por ejemplo, puede excluir de un inicio de sesión a otro los archivos y carpetas del software antivirus que no deben permanecer en un escritorio.

Correcciones

- En colaboración con los desarrolladores de NetApp, se ha solucionado un problema por el que las imágenes que incluyen una capa de NetApp se atascan al 100% de utilización de la CPU. (ALHELP-1508)
- Cuando las capas de usuarios están habilitadas y Windows se actualiza, las funciones del **menú Inicio** y de **búsqueda** de Windows funcionan correctamente. (ALHELP-1482)
- Cuando crea una capa de sistema operativo y una capa de plataforma e instala Citrix Virtual Delivery Agent (VDA), la imagen publicada ya no genera una pantalla azul. (ALHELP-1485, ALHELP-1486)
- Se ha solucionado el problema con MediTech Expanse después de actualizar el dispositivo de App Layering. (ALHELP-1494)
- Se ha solucionado el problema que impedía la configuración y el uso correctos de Dropbox en una capa de usuarios. (ALHELP-1416)
- Se ha solucionado el problema por el que el índice de búsqueda de Windows se dañaba al crear una capa de sistema operativo o al agregarle una versión. (ALHELP-1433, ALHELP-1453)

Función Labs

Las funciones de Labs son vistas previas de la funcionalidad potencial. Mientras una función esté en Labs, no la utilice en producción. No hay garantía de que esta función se incluya en el producto ni de que funcione de la misma manera si lo está.

- **Puede asignar capas de aplicación como capas elásticas en imágenes que utilizan una capa de sistema operativo diferente:** las asignaciones de capas elásticas normalmente requieren que la capa de aplicación asignada utilice la misma capa de sistema operativo que se utilizó para crear la capa de aplicación. Puede intentar asignar una capa de aplicación como [capa elástica](#) en una imagen en capas que utiliza una capa de sistema operativo diferente.

Importante:

Se pueden producir problemas al ejecutar una capa elástica en una capa de sistema operativo diferente a la utilizada para crearla.

Para usar una función de Labs, [habilitela](#) en la configuración del **Sistema**.

Ruta de actualización

Para conocer las últimas correcciones y funciones, incluida la compatibilidad con otros paquetes de software que utilice, le recomendamos que se mantenga actualizado con las [actualizaciones](#) de App Layering.

Puede actualizar desde cualquier versión de App Layering desde la versión 19.x hasta la actualidad.

App Layering 2107

Esta versión incluye las siguientes mejoras.

Correcciones

- Tras actualizar de vSphere 6.7 a vSphere 7.0 Update 2 o posterior, ahora puede crear capas y publicar imágenes con almacenamiento VSAN. (ALHELP-1410)
- Después de actualizar a Windows 10 1909 o 20H2, las aplicaciones de ClickOnce ahora funcionan con los discos de capa de usuario existentes. (ALHELP-1425)
- Una capa de aplicación asignada a un subconjunto de usuarios de un equipo y que contiene determinados archivos del sistema de Windows exclusivos de la aplicación ya no causa problemas a los usuarios que no están asignados a la capa. (ALHEALP-1427)

- En una imagen con EL ejecutándose, puede seleccionar el recurso compartido de administrador remoto en el que OneDrive guarda los archivos sin que la máquina falle con una pantalla azul. (ALHELP-1431)
- Cuando Elastic Layering está habilitado en una imagen, un script que instala una aplicación en la imagen se completa según lo previsto. (ALHELP-1432)

App Layering 2106

Esta versión incluye la siguiente función nueva:

- Una versión actualizada del sistema operativo Machine Tools. Le recomendamos que actualice las capas de su sistema operativo con las nuevas herramientas ahora, para poder usar cualquier nueva función que las requiera en el futuro.

Correcciones

- Después de finalizar una capa de plataforma, la máquina ya no falla con una pantalla azul. (ALHELP-1177)
- Cuando la composición de descarga está habilitada y se [establece el tamaño predeterminado del volumen de capas elásticas](#), el tamaño de partición grabable se actualiza para todas las imágenes publicadas. (UNI-76795)
- Al iniciar sesión después de agregar capas elásticas a una imagen, los usuarios ya no reciben errores como los siguientes (ALHELP-1445):
 - “Error crítico: el menú Inicio no funciona. Intentaremos solucionarlo la próxima vez que inicie sesión”.
 - “Citrix App Layering - Error del sistema: se ha producido un error inesperado del sistema. Vuelva a intentar la operación o póngase en contacto con asistencia técnica”.
- Los archivos de una capa elástica ya no desaparecen y vuelven a aparecer en determinadas condiciones. (ALHELP-1405)
- Al usar FSLogix y OneDrive con capas elásticas habilitadas, la máquina virtual ahora puede acceder a la carpeta de perfiles de usuario a través del recurso compartido de administración (\\PCName\C\$\Users). (ALHELP-1386, ALHELP-1405, ALHELP-1431)
- Los perfiles de FSLogix ahora funcionan correctamente cuando la aplicación se instala en una capa de aplicación. (UNI-83092)

App Layering 2104

Esta versión incluye las siguientes mejoras.

Correcciones

- La sincronización de los datos de reparación de versiones de capa ahora se ejecuta más rápido. (UNI-82197, ALHELP-1385)
- El script OfficeNoReReg.cmd actualiza ahora los valores existentes. (UNI-82088)
- Al acceder a una imagen publicada que ejecuta Windows 10 1909, ya no recibe el mensaje “El servicio de perfiles de usuario no pudo iniciar sesión. No se puede cargar el perfil de usuario”. (ALHELP-1307)
- Después de instalar CrowdStrike, Edge se inicia en el primer intento. (ALHELP-1404)
- Cuando una imagen ejecuta capas elásticas y CrowdStrike, Chrome y Microsoft Teams se lanzan al primer intento. (ALHELP-1392)
- Si instalas aplicaciones que tienen archivos con componentes de nivel de arranque y CrowdStrike los etiqueta, las aplicaciones dejarán de fallar después de añadir una versión a la capa. (ALHELP-1397)

App Layering 2102

Esta versión incluye soporte para las siguientes mejoras:

- Ahora App Layering está disponible en Google Cloud. Puede hacer lo siguiente:
 - Instale un dispositivo App Layering en Google Cloud.
 - Cree configuraciones de conectores para Google Cloud y creación de máquinas para Google Cloud.
 - Cree capas en Google Cloud.
 - Mueva capas de una plataforma diferente a Google Cloud mediante la función Exportar e importar.
 - Publique imágenes en capas en Google Cloud o en Creación de máquinas que se ejecuta en Google Cloud.

Correcciones

- Las aplicaciones publicadas a partir de una plantilla de imagen con capas elásticas habilitadas ahora se inician según lo previsto. (ALHELP-1306, ALHELP-1315, UNI-81247)

- Al arrancar un host de sesión con UEFI y Citrix Provisioning, la sesión ya no falla con una pantalla azul en el dispositivo de destino. (UNI-80889)
- La composición ya no falla porque el CE se queda sin letras de unidad disponibles (ALHELP-1286, UNI-80179)
- Cuando se instala una aplicación en una máquina empaquetadora, MSIEXEC.EXE ya no elimina los permisos sobre el contenido de syswow64. (ALHELP-1327, UNI-81548)
- WebEx ya no falla con el error 1407 al intentar desinstalarlo de una capa de usuarios. (ALHELP-1339, UNI-81434)
- Las aplicaciones del menú Inicio de Windows se enumeran en la sección correcta en lugar de en una sección con el nombre **ms-resource:*AppName*** cuando las capas de usuarios están habilitadas. (ALHELP-1323, UNI-81402)
- Al iniciar sesión en la consola de administración de App Layering ya no se producirá un error del sistema. (ALHELP-1332, UNI-81391)
- Los VDA ya no fallan con una pantalla azul en App Layering 20.11. (ALHELP-1337, UNI-82008)
- El VDA ya no deja de responder cuando los usuarios inician sesión en el VDA con Elastic Layering habilitado. (ALHELP-1369, UNI-81777)
- La creación de máquinas para el conector de vSphere ya no elimina los archivos de UnideskCacheddisks en VMware. (ALHELP-1345, UNI-81662)
- Cuando se le asigna una capa de usuarios, ya no aparece ningún error al acceder a la ficha Directiva de Studio. (ALHELP-1355, UNI-81749)

App Layering 2011

Esta versión incluye soporte para las siguientes mejoras:

- Ahora admitimos la versión 5.18 de Nutanix.
- Puede usar Windows 10, versión 20H2, como capa de sistema operativo en App Layering versión 2011 y posteriores. Sin embargo, se aplica la siguiente advertencia.

Advertencia:

Si actualiza la capa del sistema operativo a Windows 10 20H2 desde una versión anterior, actualice directamente a la compilación 19042.630 o superior. La actualización a versiones de Windows 10 20H2 publicadas antes del 16/11/2020 puede dar lugar a implementaciones de imágenes incoherentes. Por ejemplo, si publica imágenes con una plantilla con la opción **Generalizar sin conexión** seleccionada, es posible que las imágenes publicadas no funcionen correctamente.

Correcciones

- **Tiempos de inicio de sesión de Windows 10, 2004.** Se ha solucionado un problema por el que Windows 10 2004 tardaba entre 2 y 4 minutos en iniciarse y ocasionalmente incluía pantallas negras durante 30-45 segundos. (UNI-80656)
- **script kmssetup no agregado a la carpeta de scripts de inicio.** Se ha corregido un problema que impedía agregar el script kmssetup.cmd a la carpeta de scripts de inicio al descomprimirlo. (ALHELP-1279, UNI-80410)
- **El controlador HP UPD no está disponible como controlador de impresora.** Al incluir un controlador UPD de HP en una capa de aplicación que pasa a formar parte de una imagen publicada, el controlador ahora está disponible como controlador de impresora. Se ha solucionado el problema que impedía que el controlador aparezca en la lista. (ALHELP-1278, UNI-80426)
- **Las sesiones se cuelgan durante minutos.** Se ha corregido un problema que provocaba que las sesiones se bloquearan durante minutos. Este problema apareció después de actualizar a App Layering 2005. (ALHELP-1263, UNI-80262)
- **El usuario no puede volver a conectarse a su escritorio en App Layering 2009.** Se ha solucionado un problema que provocaba pantallas azules ocasionales aleatorias cuando los usuarios intentaban volver a conectarse a sus escritorios. (ALHELP-1317, UNI-81156)
- **Al usar la consola en una pantalla 4K, los diálogos se abren en la esquina superior izquierda.** Se ha solucionado el problema que provocaba que los diálogos se mostraran fuera del centro. (ALHELP-1309,UNI-78951, UNI-78952)

App Layering 2009

Esta versión incluye soporte para las siguientes mejoras:

- Ahora puede anular la ruta de acceso y el tamaño de capa predeterminados del repositorio para las capas de usuarios mediante la configuración de directivas de Citrix Studio.
- La interfaz de usuario de la consola de administración de App Layering se ha actualizado con las nuevas imágenes de marca de Citrix.

App Layering 2008

Esta versión habilita estas funciones y mejoras:

- **Compatibilidad con Windows 10, 2004:** Windows 10, 2004 ahora es compatible como sistema operativo para imágenes en capas. El uso de Windows 10, 2004 requiere App Layering versión 2008 o posterior. Los cambios necesarios para esta versión de Windows 10 no se encuentran en versiones anteriores de App Layering.

- **Compatibilidad con Citrix Hypervisor 8.2** Ahora admitimos Citrix Hypervisor versión 8.2.

Importante:

App Layering 20.8.3 incluye una actualización importante de los controladores incluidos. Si está utilizando un arranque seguro, ¡debe actualizar a la versión 20.8.3!

Los paquetes de instalación y actualización 20.8.3 están disponibles para su descarga. Para nuevas instalaciones, descargue el paquete de instalación del equipo. Para obtener actualizaciones, descargue el paquete de actualización del dispositivo.

Correcciones

- **La máquina virtual de vSphere con capas elásticas habilitadas ya no falla después de implementarse en un servidor de Citrix Provisioning.** Se ha solucionado un problema que provocaba que una máquina virtual de vSphere con capas elásticas habilitadas fallara tras implementarse en un servidor de Citrix Provisioning. (ALHELP-1202, UNI-76300)
- Se ha corregido un problema que provocaba que el instalador de AutoDesk 2020 fallara en una capa de aplicación. (ALHELP-476)
- Los usuarios ahora pueden sincronizar sus archivos de OneDrive sin problemas cuando la **sincronización On Demand** y **las capas elásticas** están habilitadas (ALHELP-468)
- Las extensiones de Chrome ya no provocan el mensaje de error “FAILED_TO_COPY_EXTENSION_FILE_TO_TE” cuando las capas elásticas están habilitadas y se asigna una capa de aplicación. (ALHELP-419)

App Layering 2005

La versión App Layering 2005 incluye compatibilidad con las siguientes funciones y mejoras:

- **Mejoras de seguridad: las mejoras** de seguridad incluyen actualizaciones del conjunto de cifrado, actualizaciones de componentes de terceros y actualizaciones del entorno en tiempo de ejecución.
- **Compatibilidad con arranque seguro:** Los controladores invitados están certificados mediante el programa **WHQL** de Microsoft. Puede utilizar controladores invitados certificados en configuraciones de arranque seguras. (UNI-74917)
- **Ruta de la capa de usuarios del cliente:** Los archivos de capa de usuarios ahora se pueden almacenar en recursos compartidos de red cuyas ubicaciones se especifican mediante rutas personalizadas. Las rutas de acceso personalizadas pueden incluir variables de entorno. (UNI-78291)

- **Aplicaciones con servicios en capa de usuarios:** cuando una aplicación instalada en una capa de usuarios contiene servicios de Windows, como Google Chrome, esos servicios se inician según lo previsto cuando el usuario inicia sesión. (UNI-77660)
- **Paquete de actualización de 2005:** El paquete de actualización de App Layering 2005 es lo suficientemente grande como para que los dispositivos antiguos no puedan descargarlo automáticamente. Si ejecuta la versión 1911 o anterior, descargue el paquete manualmente desde el [sitio de descargas](#). Además, se recomienda ejecutar la actualización desde una consola de administración en HTTP seguro (HTTPS). Si actualiza mientras está en HTTP, los mensajes no se muestran en el explorador. Si eso sucede, actualice el explorador después de 20 minutos (La actualización no causará problemas a pesar del mensaje que dice que no se actualice). Si la actualización aún se está ejecutando, obtendrá un error “servicio no disponible”. Puede ignorar ese mensaje y seguir actualizando el explorador cada pocos minutos hasta que aparezca la página de inicio de sesión.

Correcciones

- Al utilizar la composición de descarga con VMware vSphere, puede usar nombres de capas que comiencen por corchetes [], **siempre y cuando siga el corchete de cierre con un espacio**. Por ejemplo, el nombre **[SO] Windows 10** funciona, pero el nombre **[OS] Windows 10** se bloquea en vSphere studio y se agota el tiempo de espera transcurridos unos 40 minutos. (UNI-78452)

App Layering 2003

Esta versión incluye lo siguiente:

- Ahora admitimos las siguientes versiones de software de Hypervisor, Provisioning y broker de conexiones:
 - Citrix Hypervisor 8.1
 - Nutanix AOS 5.16
- Cuando los administradores configuran un tamaño de capa de usuarios predeterminado mayor, el disco se expandirá automáticamente la próxima vez que el usuario inicie sesión.
- Al crear la capa del sistema operativo en MS Hyper-V o VMware vSphere, ahora puede importar la imagen del sistema operativo mediante un script en las herramientas de máquinas del sistema operativo. El script importa la imagen del SO directamente desde la máquina virtual, en lugar de utilizar la consola de administración y la configuración del conector. El script utiliza la función Composición de descarga, que acelera la importación y permite utilizar una variedad más amplia de máquinas virtuales, incluidas las máquinas basadas en UEFI.

Correcciones

- El servicio Guest Layering (**ULayer**) se ha modificado para no depender del servicio Servidor que se ejecuta en las máquinas virtuales de los usuarios finales. (UNI-77242)
- Cuando se entrega como una capa elástica, la aplicación Artiva ya no falla cuando los usuarios intentan iniciar sesión. (UNI-76487)
- Se ha solucionado un problema que provocaba que el script `StartCCMEXEC.cmd` creciera continuamente el archivo de registros, `StartCCMExec.txt`, incluso cuando `CCMExec` no estaba instalado. Para aplicar la corrección, descargue la nueva carpeta OS Machine Tools para 20.3 y sustituya el archivo `StartCCMEXEC.cmd` por la nueva versión. (UNI-77471)
- Cuando los usuarios instalan fuentes en una capa de usuarios o capa elástica, las fuentes persisten la próxima vez que inicien sesión. (UNI-63839)
- Cuando se utiliza un conector con la **composición de descarga** habilitada para publicar una imagen, los nombres de archivo 8.3 ya no se modifican incorrectamente. (UNI-76961)
- Al agregar una versión a una capa de aplicación, ya no recibirá el error “La operación falló debido a que falta un archivo. No se encontró VMDK.”(UNI-77702)
- Se ha solucionado el problema con la expiración de los tokens web JSON (JWT) al usar la función de composición de descarga en la configuración del conector. (UNI-76859)
- El conector de Hyper-V ahora informa del tamaño del archivo de disco en lugar de su tamaño lógico, que estaba llenando rápidamente la caché. (UNI-76692)
- Se ha mejorado la compatibilidad con las directivas de GPO de Citrix Studio cuando se utilizan imágenes con capas de usuarios. (UNI-76918)

App Layering 2001

Esta versión incluye lo siguiente:

- Ahora admitimos las siguientes versiones de software de Hypervisor, Provisioning y broker de conexiones:
 - Citrix Provisioning versión 1912
 - Citrix Virtual Apps and Desktops versión 7 1912
- Las siguientes versiones de Windows 10 ahora se admiten como capa de SO:
 - Windows 10, versión 1909
 - Windows 10, edición Enterprise Virtual Desktop (disponible solo en Microsoft en Azure)
- Nuestro conector de VMware vSphere ahora es compatible con VMware Paravirtual SCSI Controller. (UNI-75620)

Correcciones

- En nuestro script de implementación de App Layering Appliance (ELM) para Azure, hemos ampliado las fechas de caducidad de las URL de Azure firmadas que apuntan a discos de repositorio estándar. Asegúrese de actualizar los scripts de implementación de Azure desde esta versión en consecuencia.
- Las instalaciones de VDA ya no fallan en una máquina de empaquetado. (UNI-76299)
- Cuando se reinicia, una imagen en capas con una capa de usuarios ya no elimina las tareas del programador. (UNI-77084)

App Layering 1911

Esta versión incluye lo siguiente:

- Ahora admitimos las siguientes versiones de software de Hypervisor, Provisioning y broker de conexiones:
 - XenApp y XenDesktop 7.15 LTSR CU5
- VMware vSphere:
 - Utilice la nueva opción de composición de descarga para reducir significativamente el tiempo que tarda en empaquetar capas y publicar imágenes.
 - Seleccione discos aprovisionados ligeros y opciones UEFI (sin arranque seguro con capas elásticas y capas de usuarios).
 - Utilice el conector de vSphere para empaquetar capas y publicar imágenes en VMware Cloud on AWS.

Correcciones

- Se ha corregido un error al finalizar las capas del sistema operativo con particiones MBR después de una actualización importante de Windows 10. (UNI-76210)
- Se ha mejorado la compatibilidad con Microsoft System Center Configuration Manager (SCCM). (UNI-76198, UNI-76126, UNI-76129)
- Los usuarios ya no pierden su conexión con un host de sesión en el que FSLogix se está ejecutando y la capa elástica está habilitada. (UNI-73793)
- Rapid Reader 8.3 ahora comienza como se esperaba después de haber sido instalado en una máquina de empaquetado. (UNI-76316)
- IntelliJ IDEA Ultimate ya no congela el escritorio cuando se inicia la aplicación. (UNI-76075)
- Los usuarios ya no reciben una pantalla azul cuando abren SQL Management Studio e intentan guardar una consulta en OneDrive o en una carpeta de SharePoint. (UNI-76427)

App Layering 1910

Esta versión incluye lo siguiente:

- Admite las siguientes versiones nuevas de software de Hypervisor, Provisioning y broker de conexiones:
 - Citrix Virtual Apps and Desktops versión 7 1909
 - Citrix Provisioning versión 1909
 - Nutanix Acropolis Hypervisor (AHV) versión 5.11
 - VMware Horizon View 7.9
- En la plataforma Hyper-V, puede empaquetar capas y publicar imágenes mediante **Compositing de descarga** para mejorar drásticamente el rendimiento y la compatibilidad. Ahora se admiten las máquinas virtuales Gen2 y los formatos de disco VHDX.
- El agente de App Layering se ha actualizado para admitir la nueva función de composición de descarga. Si utiliza el agente en la implementación, se recomienda encarecidamente que instale la actualización del agente en cualquier servidor en el que esté instalada.
- El rendimiento del índice de búsqueda de Windows se mejora cuando se utilizan capas de usuarios completas.
- Para los administradores que publican imágenes en capas, esta versión agrega validación y advertencias para proporcionar orientación sobre el tamaño del disco que se va a utilizar en función de las capas de aplicaciones seleccionadas.

Correcciones

- Se ha actualizado un artículo de asistencia de PVS que solicitaba la eliminación de la entrada del Registro de controladores CDF para solucionar problemas de Profile Management. (UNI-75720)
- Se ha solucionado el problema por el que Defender no se actualizaba correctamente. (UNI-74918)
- El servicio de búsqueda de Windows se inicia como se esperaba en una máquina de empaquetado cuando se usa un conector de almacenamiento en caché. (UNI-75915)
- Windows Defender ahora se inicia correctamente en una capa de aplicaciones creada a partir de una capa del sistema operativo Windows 1809. (UNI-74997)
- Los usuarios ahora pueden sincronizar sus archivos de OneDrive cuando la sincronización On Demand y las capas elásticas están habilitadas. (UNI-74618)
- La función bajo demanda de OneDrive ahora transmite archivos correctamente cuando las capas elásticas están habilitadas. (UNI-73121)
- Las reparaciones de la capa de usuarios ahora se completan correctamente cuando se establecen los permisos mínimos recomendados en la ruta Usuarios\. (UNI-75552)

- Al instalar una extensión de Chrome con las capas de usuarios habilitadas y una capa de aplicaciones asignada como capa elástica, ya no recibe el error `Can not install package: FAILED_TO_COPY_EXTENSION_FILE_TO_TEMP_DIRECTORY` (UNI-75568)
- Se ha mejorado el rendimiento del índice de búsqueda de Windows cuando se utilizan capas de usuarios completas. (UNI-73049)
- Esta versión agrega validaciones y advertencias sobre el tamaño de disco que puede usar. La guía se basa en su configuración y en las capas de aplicación seleccionadas. (UNI-54390)

App Layering 1908

Esta versión habilita estas nuevas funciones y mejoras.

- **Versiones de Windows:** Windows 10 versión 1903 ahora es compatible como capa de sistema operativo.
- **Brokers de conexión:** Ahora admitimos la siguiente versión de software de agente de conexión:
 - VMware Horizon View 7.9
- **Reparación de capas de usuarios:** ahora puede reparar manualmente las capas de usuarios para que todos los archivos y la configuración del registro provenientes de un conjunto específico de capas de aplicaciones puedan volver a ser visibles.

Correcciones

- Las sesiones de PowerShell del conector de Hyper-V ya no caducan cuando una copia de archivo tarda más de 30 minutos. (UNI-74283, UNI-74292)
- Se ha solucionado el problema por el que las propiedades Sistema y Visualización no se abran correctamente cuando se habilitaron las capas de usuarios. (UNI-74547)
- La eliminación de aplicaciones de almacén de una capa del sistema operativo Windows 10 ya no provoca el mal funcionamiento de funciones, como **Configuración** y **Propiedades de pantalla**. (UNI-74852)
- La actualización KB4052623 de Windows Defender ahora se instala correctamente y funciona para usuarios habilitados para capas de usuarios. (UNI-74942)

Contactar con Citrix

Agradecemos sus comentarios sobre esta versión.

- Utilice nuestro Foro en línea para hablar directamente con los empleados de Citrix y otras organizaciones que implementan Citrix App Layering.

- Para problemas y preguntas sobre productos, abra un caso de asistencia.

Esperamos escuchar lo que piensa sobre App Layering.

Información relacionada

- [Support Knowledge Center](#)
- [Enterprise Architect TechTalks: Preguntas frecuentes sobre Citrix App Layering](#)
- [Discusiones de Citrix App Layering](#)
- [Instrucciones sobre App Layering](#)

Elementos retirados

January 12, 2024

Los anuncios de este artículo son avisos avanzados de las funciones de Citrix App Layering que se están eliminando gradualmente para que pueda tomar decisiones empresariales oportunas. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas. Para obtener información detallada sobre el ciclo de vida útil de los productos, consulte el artículo [Product Lifecycle Support Policy](#).

Elementos eliminados y obsoletos

La siguiente lista muestra las funciones de Citrix App Layering que están en desuso o se quitan.

Los elementos *retirados* no se eliminan inmediatamente. Citrix sigue ofreciendo los elementos retirados hasta eliminarlos en una versión futura.

Los elementos *eliminados* se eliminan o ya no se admiten en Citrix App Layering.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Capa de usuarios de sesión de Office 365/Office 365	Ha quedado obsoleta la compatibilidad con Office 365 como selección para el tipo de capa de usuarios.	Agosto de 2023	Objetivo: primer trimestre de 2024	Utilice Citrix Profile Management para casos de uso avanzados de Office 365.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Compatibilidad con VMware vSphere 6.7	Se eliminó la compatibilidad con VMware vSphere 6.7.		Junio de 2023	Utilice versiones posteriores de VMware vSphere .
conector de Azure	Soporte obsoleto para el conector de Azure antiguo.	Noviembre de 2022	Objetivo: Cuarto trimestre de 2023	Utilice el conector de Azure Deployments , que se incluye con App Layering 2211.
Conector de VMware Horizon View	Soporte obsoleto para el conector de VMware Horizon View	Marzo de 2022	Q3 2022	Diciembre de 2023

Problemas conocidos

June 27, 2024

Actualización de versiones de App Layering

App Layering 2312

Es posible que no se pueda actualizar a App Layering 2312 y se devuelva el error «Se ha producido un error al actualizar el dispositivo». Vuelva a intentar la actualización después de volver de una instantánea limpia”. Somos conscientes de un problema con algunos dispositivos que se actualizaron desde versiones anteriores. En este escenario, la actualización podría fallar debido a la presencia de componentes del actualizador heredados. Estamos trabajando en una compilación parcheada para App Layering 2306 que contiene una solución permanente para este problema.

Para solucionar este problema, es necesario eliminar el módulo antiguo realizando los siguientes cambios en el dispositivo Layering:

1. Inicie sesión en la consola del dispositivo con el nombre de usuario y la contraseña raíz.

2. Ejecute el comando “yum remove mod_http2”. El comando puede tardar varios minutos en ejecutarse.
3. Una vez completado el comando, vuelva a iniciar sesión en el dispositivo mediante un explorador web y vuelva a ejecutar la actualización.
4. La actualización puede tardar 30 minutos o más en completarse, pero ahora debe realizarse correctamente.

App Layering 2005

- El paquete de actualización de App Layering 2005 es lo suficientemente grande como para que los dispositivos antiguos no puedan descargarlo automáticamente. Si ejecuta la versión 2001 o anterior, descargue el paquete manualmente desde el [sitio de descargas](#).
- Se recomienda ejecutar la actualización desde una consola de administración en HTTP seguro (HTTPS). Si actualiza mientras está en HTTP, los mensajes no se muestran en el explorador. Si eso sucede, actualice el explorador después de 20 minutos (La actualización no causará problemas a pesar del mensaje que dice que no se debe actualizar). Si la actualización sigue ejecutándose, aparece el error “servicio no disponible”. Es seguro ignorar el mensaje y seguir actualizando el explorador cada pocos minutos hasta que aparezca la página de inicio de sesión.
- Si tiene dos paquetes de actualización con el mismo nombre en carpetas diferentes en el recurso compartido de archivos de red, al seleccionar uno de esos paquetes, se seleccionarán ambos paquetes. Si ambos paquetes tienen la misma versión, la actualización se realiza correctamente. Si tienen versiones diferentes, el sistema elige el número de versión inferior. Esto ocurre con Enterprise Layer Manager (ELM) versión 22.2.

Dispositivo de App Layering y consola de administración

- En la nueva interfaz de usuario, los tipos de plataforma no se pueden modificar. **Modificar tipos de plataforma** sigue funcionando correctamente en la interfaz de usuario anterior. (UNI-86856)
- Al instalar el dispositivo de App Layering, *debe* usar la configuración de CPU predeterminada de **4 CPU**.
- Si utiliza roles en un entorno complejo de Active Directory y los inicios de sesión son lentos, asigne todos los roles a usuarios explícitos en lugar de a grupos.

Enlaces a la documentación de App Layering

Los vínculos de documentación de la consola de administración se abren como una página en blanco en Internet Explorer 11. Para solucionar este problema, pega el enlace en otro explorador. La documentación se muestra correctamente.

Agente de App Layering

De forma predeterminada, el agente de Citrix App Layering se ejecuta en la cuenta **del sistema local** en el servidor Hyper-V. Si cambia la cuenta a otra que no sea **Sistema local**, el agente no puede transferir discos desde y hacia el dispositivo.

App Layering OS Machine Tools

- (Solo versión 19.5) Después de actualizar a la versión 19.5 (o posterior) desde 19.3 (o anterior), asegúrese de actualizar Activación de KMS Office para usar Office 2019. Al preparar la imagen del sistema operativo para la creación de capas, descargue y ejecute las nuevas herramientas de máquina con sistema operativo de App Layering.
- (Solo en la versión 19.1) Al preparar la imagen del sistema operativo para la creación de capas, asegúrese de que la activación de KMS Office se active al iniciar el escritorio. Solo para esta versión, descargue y ejecute App Layering OS Machine Tools desde la **versión 18.12**.

Microsoft Teams 2.x

Microsoft Teams 2.x ha cambiado su método de instalación y ahora se instala en `C:\Program Files\WindowsApps`. Para admitir este cambio, debe ejecutar la versión 2403.2 o posterior de App Layering. Puede descargar un disco de actualización en la página de [descargas de App Layering](#) que incluya esta corrección.

Tenga en cuenta lo siguiente:

- Aún debe seguir las recomendaciones de MSFT para impedir que ciertas carpetas o archivos persistan.
- Elastic-fit indica que estas capas de aplicaciones no son adecuadas para la asignación elástica (incluye las capas de aplicaciones UWP/AppX en la imagen publicada).
- Los usuarios actuales de la capa de usuarios pasan por una experiencia de inicio de sesión “por primera vez” si se realizan cambios en la combinación o si se modifican las versiones de estas dos aplicaciones en la imagen.
- Al actualizar Microsoft Teams en una revisión de la capa de aplicaciones, quite la versión anterior antes de instalar la versión más reciente.
- Si Microsoft Teams 2.1 se instaló anteriormente en la capa del sistema operativo, se debe quitar de la capa del sistema operativo antes de crear capas de aplicaciones.

Si está ejecutando una versión anterior de App Layering, se necesita una solución alternativa para instalar Microsoft Teams 2.1 en la capa del sistema operativo. Use la siguiente solución temporal.

Solución temporal:

1. Cree una versión de capa de sistema operativo.
2. Descargue el instalador .exe para Windows 10 u 11.
3. Descargue MSIX.

Nota:

Para obtener más información sobre el instalador .exe y MSIX, consulte la documentación de [Microsoft](#).

4. Abra una línea de comandos de administrador.
5. Deshabilite la actualización automática de Microsoft Teams con el siguiente comando:

```
reg add hklm\software\microsoft\teams /v disableAutoUpdate /t REG_DWORD /d 1 /f
```
6. Según la ubicación de su `.MSIX`, siga los siguientes pasos:
 - a) Para Windows 10 u 11, usa el siguiente comando: `.\teamsbootstrapper.exe -p -o "c:\path\to\teams.msix"`
 - b) Para Windows Server 2016, 2019 o 2022, usa el siguiente comando: `Dism /Online /Add-ProvisionedAppxPackage /PackagePath:<MSIX package path> /SkipLicense`
7. Para completar la instalación, inicie Microsoft Teams.
8. Cree un archivo `UserExclusion` para incluir las siguientes exclusiones recomendadas por MSFT:
 - `c:\Users*\AppData\Local\Publishers\8wekyb3d8bbwe\TeamsSharedConfig\Meeting-Addin\`
 - `c:\Users*\AppData\Local\Packages\MSTeams_8wekyb3d8bbwe\LocalCache\Microsoft\MSTeams\Logs\`
 - `c:\Users*\AppData\Local\Packages\MSTeams_8wekyb3d8bbwe\LocalCache\Microsoft\MSTeams\PerfLogs\`
 - `c:\Users*\AppData\Local\Packages\MSTeams_8wekyb3d8bbwe\LocalCache\Microsoft\MSTeams\EBWebView\WV2Profile_tfw\WebStorage\`
9. Finalice la versión de la capa del sistema operativo.
10. (Opcional) Asegúrese de que ninguna capa de aplicación que contenga una versión anterior de Microsoft Teams esté asignada de forma elástica o estadística.

Nota:

- No ejecute el archivo `.MSIX` en sí. Esto instala Microsoft Teams y estaría disponible en el menú Inicio, pero al hacer clic en él, el proceso no se inicia.

- No inicies sesión en ninguna cuenta de Microsoft Teams mientras creas una capa de sistema operativo y no cambies ninguna configuración de Microsoft Teams.
Las cuentas personales no son compatibles con los nuevos Microsoft Teams.
Para obtener más información, consulte la documentación de [Microsoft](#).

[UNI-90395]

Capas elásticas

- Microsoft Office no puede tener capas *elásticas* debido a la forma en que sus licencias se integran con la Tienda Windows. La capa de aplicaciones de Office debe incluirse en la imagen en capas.
- Cuando habilita una imagen con capas elásticas, es posible que los usuarios puedan ver archivos y directorios de otras sesiones en el Explorador de Windows. Los directorios explorados en la otra sesión pueden crear carpetas visibles para todas las sesiones que tienen permiso para examinar ese directorio.
- Si utiliza asignaciones de capa elástica con Windows Server 2008 o Windows 7, cree el recurso compartido de archivos con un tamaño de sector de 512. Para obtener información detallada sobre este problema y las actualizaciones relacionadas del sistema operativo, consulte:
 - [Directiva de compatibilidad de Microsoft con discos duros del sector 4K en Windows](#)
 - [Actualización que mejora la compatibilidad de Win 7 y Win Server 2008 R2 con discos de formato avanzado \(UNI-48984\)](#)

Capas de usuarios

- **Al iniciar sesión después de la actualización, se inician las pantallas de Windows First Sign-in:** Cuando inicia sesión después de actualizar a 4.10 o posterior, el inicio de *sesión habitual de Windows First Sign-in* actualiza la capa de usuarios con la versión del sistema operativo. El proceso conserva los archivos de capa de usuarios.

Compatibilidad con Windows 10

- **Actualizaciones de Windows 10, versión 20H2.** Si actualiza la capa del sistema operativo a Windows 10 20H2 desde una versión anterior, actualice directamente a la compilación 19042.630 o posterior. La actualización desde compilaciones de Windows 10 20H2 publicadas antes del 16/11/2020 puede provocar implementaciones de imágenes incoherentes. Por ejemplo, si publica imágenes con una plantilla con la opción **Generalizar sin conexión** seleccionada, es posible que las imágenes publicadas no funcionen correctamente.

- **La actualización requiere pasos adicionales cuando se va a una nueva versión principal de Windows 10:** Durante la actualización, Windows 10 puede crear un volumen de recuperación en el mismo disco que la versión de la capa del sistema operativo. Elimine siempre este volumen antes de finalizar la versión de la capa de SO. De lo contrario, el volumen de recuperación puede provocar que los escritorios no se inicien correctamente. Para obtener más información, consulte Issue 9 en [Windows 10 v2004, 20H2, 21H1 y 21H2: problemas conocidos de Citrix](#).
- Si ha generado y aplicado el script `Optimizations.cmd` de App Layering a una capa de sistema operativo Windows 10 1909, es posible que la opción **Buscar** en el menú **Inicio** no funcione como se esperaba. Para evitar este problema, agregue una versión a la capa del sistema operativo y ejecute el programa `c:\windows\setup\scripts\Optimize.hta`. Para crear otro script `Optimizations.cmd` para aplicarlo a la nueva versión de capa, anule la selección de **Inhabilitar el servicio de entrada de tableta (Sección 6, Opción M)** y seleccione **Guardar archivo**. Antes de finalizar la capa de SO, ejecute el comando `Powershell Set-Service TabletInputService -startuptype manual` para deshacer el efecto de cualquier anterior `Optimizations.cmd` que pudiera haber inhabilitado el servicio.

Conectores

- Al utilizar el conector de **implementaciones de Azure**, si elimina todas las plantillas y modifica el conector para elegir una plantilla nueva, aparecerá una versión de la plantilla eliminada. A continuación, al hacer clic en **Guardar**, aparece un error. Como solución alternativa, vuelva a seleccionar una versión de plantilla válida antes de hacer clic en **Guardar**. (UNI-88412)
- Al utilizar la opción de disco de arranque mini de Windows, puede especificar hasta cuatro capas de requisitos previos para cualquier capa de aplicaciones determinada. Si una aplicación requiere que haya más de cuatro aplicaciones más durante la instalación, instale varias aplicaciones en una capa. (UNI-69524)
- Al crear una capa (aplicación, sistema operativo o plataforma) en Windows 7 **de 64 bits**, si **selecciona Descargar composición en** la configuración del conector, puede tener problemas para agregar una versión a la capa. Se produce un error y no se crea la máquina de embalaje. Cuando *no* se selecciona Compositing de descarga en la configuración del conector, se crea la máquina de embalaje. (UNI-82545)
- Recibir el error 503, “Problemas de servidor ocupado” de Azure. Si recibe este error de forma constante, siga los pasos de [CTX310868](#). Este problema ocurre esporádicamente y se está probando una solución para ello. (ALHELP-1383)
- Si intenta introducir un nombre para un conector y ese nombre ya existe, recibirá un mensaje de error genérico del sistema, en lugar del mensaje de error correcto. El problema se produce en los conectores **Azure Deployments**, **Machine Creation for Azure Deployments**, **VMware vSphere** y **Machine Creation for vSphere**. (UNI-89218)

Citrix Provisioning

- Al crear una plantilla de imagen, la configuración del hardware del dispositivo de destino debe coincidir con la configuración del sistema operativo Windows y de la capa de plataforma. Asegúrese de que la configuración de hardware en el dispositivo de destino coincida con la configuración de hardware del sistema operativo y de la capa de plataforma, especialmente el número de CPU. Si la configuración no coincide, aparecerá el mensaje «es necesario reiniciar» al iniciar la imagen publicada. (UNI-50799)
- Si usa Provisioning Services, debe inhabilitar IPv6 en la capa del sistema operativo y *no* en la capa de la plataforma. (UNI-53600)
- Al importar archivos VHDX publicados desde App Layering al almacén de discos PVS, a veces recibe un mensaje de disco no válido. Elimine el error cambiando los caracteres de punto (.) en la fecha y hora del nombre de archivo publicado. Un nombre de archivo válido contiene solo un punto para la extensión de archivo VHDX. (UNI-75902)
- Cuando se selecciona **Compositing de descarga** en la configuración del conector:
 - La ruta del almacén de Citrix Provisioning no se valida si contiene espacios. Reemplace los espacios por **%20** para que el nombre sea válido. (UNI-84868)
 - Los trabajos de publicación fallan si la ruta del recurso compartido de archivos termina con una barra invertida (\). (UNI-85045)
 - Los trabajos de publicación fallan con un mensaje de error ComponentActivator si el usuario del dominio no tiene permiso de lectura y escritura en la ruta del recurso compartido de archivos. (UNI-85020)
- Cuando selecciona un conector de Hyper-V para la configuración de composición de descarga y la capa del sistema operativo es Gen 2, debe crear otra versión de la capa del sistema operativo y, a continuación, crear la capa de plataforma a partir de esa versión del sistema operativo. De lo contrario, el objetivo no arranca. (UNI-85044)
- Al establecer la ruta del recurso compartido de archivos de composición para la configuración del conector, no se verifica la conectividad entre el motor de composición y el almacén de Citrix Provisioning. Si la ruta del almacén no se asigna a la ruta del recurso compartido de archivos, recibirá un error similar al siguiente:
 - Error: “Se ha producido un error inesperado del sistema. Reintente la operación o póngase en contacto con el soporte técnico. Mensaje de excepción: el código de estado de respuesta no indica éxito: 404 (no encontrado). [Detalles de excepción] (UNI-85045), (UNI-85020)

XenServer

- Cuando prepare la imagen del sistema operativo para usarla en XenServer, debe abrir el puerto 5900 para permitir el acceso a la consola. (UNI-50846)
- Establezca siempre la configuración del conector de Citrix App Layering para que apunte al nodo maestro. (UNI-52454)
- Capas de requisitos previos:
 - Si una máquina se cuelga al arrancar y se selecciona una capa de requisitos previos, es probable que uno de los discos de capa no esté conectado. Asegúrese de que Citrix Guest Tools esté incluido en las capas del sistema operativo o de la plataforma.
 - Si utiliza capas de requisitos previos para crear el SO o la capa de plataforma, Citrix Tools debe estar presente. Sin las herramientas, la máquina de embalaje falla y recibe una pantalla azul. XenServer no puede ver ningún dispositivo conectado *después* de la unidad de DVD. La unidad de DVD está siempre en la tercera ranura. (UNI-67741)

Citrix Virtual Apps and Desktops (CVAD)

- Al actualizar Citrix Virtual Apps and Desktops a la versión 7.15 CU4, primero debe instalar .NET Framework 4.7.1 en una nueva versión de la capa de sistema operativo, en lugar de en la capa de plataforma. La instalación de .NET Framework 4.7.1 en la capa del sistema operativo garantiza que todas las capas de aplicaciones, capas de plataforma e imágenes funcionen correctamente. Las actualizaciones más recientes de Windows ya incluyen .NET Framework 4.7.1 como parte de las actualizaciones. (ALHELP-588, UNI-75108)

Google Cloud

- Al importar capas desde otra plataforma, debe agregar una versión a la capa del sistema operativo y cambiar a usar la nueva versión de la capa a partir de ese momento. De lo contrario, es probable que las máquinas de embalaje y las imágenes publicadas fallen con una pantalla azul.
- Configuración de Google Cloud Connector. «Comprobar credenciales» verifica el rol de usuario de la cuenta de servicio. Si la cuenta de servicio especificada en el **archivo de clave JSON de la cuenta de servicio** de configuración de Google Cloud connector es diferente a la cuenta de servicio asociada a la **plantilla de instancias** seleccionada, la cuenta de servicio en la configuración debe tener el **usuario de la cuenta de servicio** papel. Si no es así, recibirá un error al implementar una máquina con esa configuración de conector. (UNI-82082)

Nutanix Acropolis

- El siguiente mensaje durante la creación de capas de aplicaciones indica que la configuración de capa de aplicaciones especifica una capa de plataforma. No utilice capas de plataforma con la función de almacenamiento en caché de la capa de aplicaciones que mejora el rendimiento. (UNI-67742)

Create Application Version Wizard - Confirm and Complete

Verify the version details are correct and click Add Version to create a new version for the App Layer



By selecting a platform layer packaging performance will be degraded

VMware vSphere

- Al crear la capa del SO mediante el Asistente para crear capa de SO, se muestran las máquinas virtuales de la interfaz unificada de firmware extensible (UEFI). Sin embargo, no puede crear máquinas UEFI mediante el asistente. En su lugar, utilice el nuevo script `ImportOsLayer.ps1` para [importar el sistema operativo](#) en la nueva máquina de capa de sistema operativo.
- Cuando se usa una configuración de conector de vSphere con VMware Cloud y un almacén de datos de vSAN 7.0 Update 2 (o posterior), se debe seleccionar **Compositing de descarga**. (UNI-85216)
- Al utilizar el nuevo conector VMware vSphere en AL 23.4, si selecciona una red opaca al crear o modificar el conector, el conector fallará. Como solución alternativa, seleccione una red no opaca. Las configuraciones de conectores existentes que utilizan una red opaca creada antes de AL 23.4 siguen funcionando normalmente. (UNI-89439)

Microsoft Azure

- App Layering no admite el almacenamiento de Azure File. Para el almacenamiento en Azure, cree un recurso compartido de archivos SMB o un recurso compartido de archivos de red. (UNI-42272)
- Los discos administrados solo se admiten con las importaciones de SO. El empaquetado de capas de aplicaciones y la publicación de imágenes solo producen discos no administrados. Al crear una máquina virtual en Azure, seleccione **Sin discos administrados**.

Microsoft Hyper-V

- Al seleccionar una configuración de conector de Hyper-V para la composición de descarga y su capa de SO es Gen 2, la capa debe tener al menos una versión además de la original. Además, la capa de plataforma en la que se instala el software del dispositivo de destino de Citrix Provisioning debe crearse con la nueva versión de la capa de SO. (UNI-85044)
- Cuando se establece una configuración de conector Hyper-V para Compositing de descarga con Gen 2 (UEFI) y VHDX, se permite elegir VHD como formato de disco en la configuración del conector de Citrix Provisioning, pero esta configuración no es compatible.
- Al configurar Elastic Layering en Hyper-V, debe usar grupos RDS *no administrados* (UNI-53545)
- Al crear una capa de aplicación, si se especifica una capa de plataforma en la configuración de la capa de aplicación, recibirá un error. No use capas de plataforma con la función de almacenamiento en caché de App Layering. (UNI-71868, UNI-67743)

Create Application Version Wizard - Confirm and Complete

Verify the version details are correct and click Add Version to create a new version for the App Layer



By selecting a platform layer packaging performance will be degraded

- Crear una capa de SO en Hyper-V Server 2019 puede dar lugar a este error:

“No se pudo crear el disco duro virtual. Asegúrese de que haya suficiente espacio en el recurso compartido especificado en la configuración del conector”.

Este error se debe a un problema con el cmdlet New-VHD de Microsoft PowerShell. Estamos vigilando una solución de Microsoft. Mientras tanto, use la siguiente solución alternativa para este error:

1. Asegúrese de que la máquina virtual dorada no tenga puntos de control.
2. Asegúrese de que el disco de máquinas virtuales Gold está en la misma ruta de directorio que está configurada en la configuración del conector. Ejemplo: ruta local es D: Brock
Gold VM disco se almacena en D:\Brock\Win10Gold\Win10GoldDisk.vhdx

- App Layering no puede crear una capa de aplicación o plataforma si la ruta de almacenamiento en la configuración del conector Hyper-V contiene una comilla invertida (‘). Por ejemplo:

```
1 mystoragename`
2 <!--NeedCopy-->
```

Impresión

Con las imágenes de App Layering configuradas para Full User Layer, puede instalar sus propios dispositivos de impresión directamente. Sin embargo, al cerrar sesión e iniciar sesión, **las impresoras y escáneres** ya no muestran los dispositivos de impresión autoinstalados.

Como solución alternativa, puede acceder a las impresoras o seleccionarlas desde las aplicaciones.

Red

Es posible que las aplicaciones que incluyen componentes de red no funcionen correctamente cuando se instalan en una capa de aplicaciones y, a continuación, se incluyen en una imagen publicada. Las aplicaciones de este tipo deben instalarse en la capa del sistema operativo o en la capa de plataforma para garantizar una combinación adecuada de la información de registro relacionada con la red en la imagen.

Información relacionada

- [Support Knowledge Center](#)
- [Enterprise Architect TechTalks: Preguntas frecuentes sobre Citrix App Layering](#)
- [Discusiones de Citrix App Layering](#)
- [Instrucciones sobre App Layering](#)

Requisitos del sistema

May 9, 2024

El dispositivo virtual App Layering se ejecuta en los hipervisores compatibles enumerados en este artículo. El dispositivo es donde se implementa Enterprise Layer Manager (ELM) durante la instalación.

Puede crear capas para utilizarlas en prácticamente cualquier Hypervisor o software de Provisioning. Para obtener la mejor experiencia de usuario, publique imágenes en las plataformas compatibles.

Hipervisores para el dispositivo

Enterprise Layer Manager (ELM) se ejecuta en un dispositivo virtual implementado en un Hypervisor compatible.

- XenServer, versiones 6.5, 7.0—7.6, 8.0, 8.1, 8.2
- Azure Resource Manager
- Google Cloud
- Microsoft Hyper-V que se ejecuta en Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 o Windows Server 2022
 - Las máquinas virtuales de generación 2 se admiten cuando se utiliza la función de composición de descarga.
- Nutanix Acropolis Hypervisor (AHV), versiones 5.0—5.5 (solo Prism Element), 5.8, 5.9, 5.10, 5.11, 5.15 (versión de soporte a largo plazo), 5.16, 5.17, 5.18, 5.19, 6.5 (versión de soporte a largo plazo)
- vSphere vCenter, versión 7.0 u 8.0 (incluidas las actualizaciones posteriores)
 - Las máquinas virtuales de segunda generación son compatibles con vSphere vCenter versión 7.0 u 8.0 (y actualizaciones posteriores) cuando se usa la función de composición de descarga

Protocolo de recursos compartidos de archivos de red

- Bloque de mensajes de servidor (SMB)

Conexión de red

- Citrix recomienda una conexión de 10 Gbps entre el dispositivo y el recurso compartido de archivos.

Servicio de directorios

- Microsoft Active Directory

Explorador de Internet para consola de administración

La consola de administración admite los siguientes exploradores web:

- Edge versión 94 o posterior (versión 102 probada oficialmente)
- Chrome (versión 90 y 102 probadas oficialmente)
- Firefox (versión 45 - 52.9 probada oficialmente)

Sistema operativo para imágenes en capas

Puede aplicar capas a las siguientes versiones del sistema operativo Windows. Las aplicaciones de Microsoft Store funcionan en todas las versiones compatibles de Windows.

- Sistemas operativos Windows Server: se admiten las siguientes versiones de host de sesión:
 - Windows Server 2022, 64 bits (ediciones Standard y Datacenter)
 - Windows Server 2019, 64 bits (ediciones estándar y de centro de datos)
 - Windows Server 2016, 64 bits (ediciones estándar y de centro de datos)
 - Windows Server 2012 R2, 64 bits (ediciones estándar y de centro de datos)
- Sistemas operativos de escritorio: se admiten las siguientes versiones de escritorio:
 - Windows 11, versión 22H2, compatible con la versión 22H1 y versiones posteriores de App Layering.
 - Windows 10, versión 22H2, compatible con la versión 22H1 y versiones posteriores de App Layering.
 - Windows 11, versión 21H2. Se admite en la versión 21H2 y posteriores de App Layering.
 - Windows 10, versión 21H2. Se admite en la versión 21H1 y posteriores de App Layering.
 - Windows 10, versión 21H1. Se admite en la versión 21H1 y posteriores de App Layering.
 - Windows 10, versión 20H2. Se admite en la versión 20H2 y posteriores de App Layering.

Advertencia:

Si actualiza la capa del sistema operativo a Windows 10 20H2 desde una versión anterior, actualice directamente a la compilación 19042.630 o posterior. La actualización a versiones de Windows 10 20H2 publicadas antes del 16/11/2020 puede dar lugar a implementaciones de imágenes incoherentes.

- Windows 10, 64 bits, versiones 2004, 1909, 1903, 1809, 1803, 1709, 1703 y 1607 (ediciones educativas y empresariales)
- Windows 10, 64 bits, versiones 2004, 1909, 1903, 1809, 1803 (edición Professional)

App Layering admite paquetes de idioma de un solo byte para el sistema operativo Windows básico de inglés de Estados Unidos. Admite paquetes de idioma de varios bytes cuando la capa del sistema operativo se implementa en versiones compatibles de:

- XenServer
- VMware vSphere
- Microsoft Hyper-V

Capas de usuarios

Las capas de usuarios completas se admiten en las siguientes plataformas:

- Sistemas operativos:
 - Windows 10, 64 bits
 - Windows 11, 64 bits (solo si se implementa en una plataforma habilitada para la composición de descarga)
- Plataformas de publicación:
 - Citrix Virtual Desktops

Imágenes en capas

Las imágenes en capas son imágenes de arranque compuestas a partir de capas. Cada imagen en capas contiene una capa de SO, una capa de plataforma y cualquier número de capas de aplicaciones. Puede publicar imágenes en capas en estas plataformas:

- Creación de máquinas para XenServer (anteriormente Citrix MCS para XenServer)
- Creación de máquinas para Azure y Azure Government
- Machine Creation for vSphere
- Machine Creation for Nutanix AHV
- Citrix Provisioning, versiones 2203, 2106, 2012, 2009, 2006, 2003, 1912, 1909, 7.15 CU6, 1912 CU3 y Provisioning Service (PVS), versiones 7.15 LTSR (cualquier versión)

Notas:

- Citrix recomienda velocidades de red de 10 Gbps para el almacén de aprovisionamiento.
- Ya no se admiten las versiones 7.1, 7.6—7.9, 7.11—7.18 y 1808 de Provisioning Service (PVS).

El dispositivo y los conectores se ejecutan en los siguientes entornos:

- Citrix Virtual Apps and Desktops, versiones 7: 1808, 1811, 1903, 1906, 1909, 1912 (LTSR, CU1-CU5), 2003, 2006, 2009, 2012, 2103, 2106, 2112, 2203 (LTSR), 2206, 2209, 2212
- Citrix XenApp and XenDesktop, versiones 6.5, 7.0—7.18, and 7.15 (LTSR, CU3 - CU7)
- Citrix Virtual Apps and Desktops Essentials para Azure
- XenServer
- Google Cloud

- Microsoft Azure
- Microsoft Hyper-V
- Nutanix Acropolis
- VMware vSphere

Provisioning de escritorios y entrega de aplicaciones

Puede usar imágenes en capas para escritorios persistentes, siempre y cuando *no* habilite las capas elásticas ni las capas de usuarios (Full u Office 365).

Para habilitar capas de usuarios o capas elásticas, *debe utilizar máquinas no persistentes*.

Nota:

Las capas elásticas no son compatibles con View Persona Management.

Funciones de App Layering por edición

Según la [tabla de funciones de Citrix DaaS y Citrix Virtual Apps and Desktops \(CVAD\)](#), Citrix App Layering está disponible en todas las ediciones. Esto significa que puede hacer lo siguiente en cualquier número de sitios Citrix DaaS y CVAD de su entorno:

- Cree un número ilimitado de capas de sistema operativo, plataforma y aplicación
- Crea un número ilimitado de imágenes en capas
- Crea un número ilimitado de capas elásticas

Planificar su implementación

June 27, 2024

En esta sección se describen los aspectos que deben tenerse en cuenta al planificar la implementación de Citrix App Layering.

dispositivo de App Layering

Puede instalar un dispositivo de App Layering en un hipervisor y utilizarlo para publicar imágenes en el mismo Hypervisor o en otro.

El dispositivo está diseñado para notificarle cuando haya una actualización disponible. El dispositivo aloja una consola de administración basada en Web donde puede administrar el sistema, incluidas las capas y las plantillas de imagen.

- **Consola de administración:** el dispositivo aloja una consola de administración que puede utilizar para crear capas para su sistema operativo, software de plataforma y aplicaciones. La consola también permite crear plantillas de imagen que especifiquen las capas que se van a incluir en las imágenes que se publiquen.
- **Copias de seguridad: recomendamos hacer copias** de seguridad de cada dispositivo para no perder las capas que dedica tiempo a crear. Necesita una copia de seguridad completa de cada dispositivo para garantizar que puede recuperar toda la información de él. Aunque puede exportar e importar capas, esta función no está diseñada para la recuperación de errores. Para obtener información más detallada sobre la disponibilidad, las copias de seguridad y la recuperación, consulte [este artículo](#) en Citrix Tech Zone.

Capas

La arquitectura de App Layering le permite administrar una sola copia del sistema operativo Windows y las aplicaciones, independientemente del hipervisor. Puede mantener un conjunto de aplicaciones para dos entornos. Por ejemplo, puede implementar un sistema operativo y sus capas de aplicaciones en un hipervisor local y en un hipervisor basado en la nube. Las mismas capas se ejecutan en cada una de ellas.

Puede crear capas para su sistema operativo, herramientas de plataforma y aplicaciones. Para conservar la configuración y los datos de los usuarios, habilite las capas de usuarios en las plantillas de imagen.

Capa de sistema operativo

La capa de SO incluye el software y la configuración del sistema operativo y del hipervisor. Es un bloque de creación esencial para todas las demás capas que cree. Solo necesita una capa de SO para un sistema operativo Windows específico. Por ejemplo, si admite tanto un SO de escritorio de Windows como un SO de servidor Windows, cree una capa de SO para cada uno. Las capas de plataforma y aplicación que cree requieren la capa del sistema operativo que utiliza para ello.

Cuando agrega una actualización a una de las capas del sistema operativo, las capas de plataforma y aplicación creadas con ese sistema operativo continúan ejecutándose en él.

Capa de plataforma

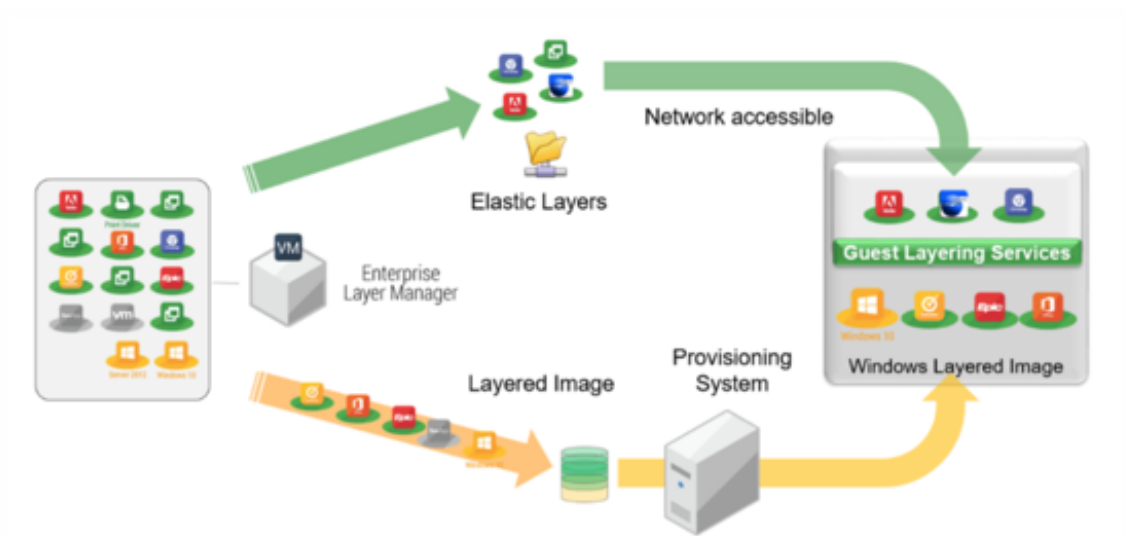
La capa de plataforma incluye el software de Provisioning y las herramientas de broker de conexión. Además, si va a publicar en un hipervisor distinto al de la capa del sistema operativo, agregue las nuevas herramientas de hipervisor a la capa de plataforma.

La capa de plataforma garantiza que las capas del sistema operativo y de la aplicación se ejecuten sin problemas en un entorno local o en la nube específico. Puede reutilizar las capas del sistema operativo y de la aplicación y seleccionar una capa de plataforma diferente para cada hipervisor o servicio de aprovisionamiento.

Capas de aplicaciones

Las capas de aplicaciones incluyen el software para cada una de sus aplicaciones. Si mantiene más de un sistema operativo, necesita un conjunto de capas de aplicaciones para cada una.

Puede implementar aplicaciones como parte de imágenes en capas o como capas elásticas. Las imágenes en capas se utilizan para aprovisionar los sistemas de los usuarios, mientras que las capas elásticas se entregan cuando el usuario inicia sesión.



Capas elásticas

Para utilizar capas elásticas necesita una imagen en capas en la que haya habilitado la capa elástica. Una estrategia típica es:

- **Implementación de imágenes en capas:** incluye las capas del sistema operativo y la plataforma, así como las aplicaciones que son para todos los usuarios. MS Office y Visual Studio *deben* incluirse en la imagen en capas y no se pueden implementar como capa elástica.
- **Capas elásticas:** habilite las capas elásticas en la plantilla de imagen y, a continuación, asigne capas de aplicación a grupos de usuarios y grupos de máquinas. Cuando la capa elástica está habilitada, los usuarios reciben capas de aplicación asignadas a ellos (el usuario), un grupo al que pertenecen o el equipo en el que están iniciando sesión.

Capas de usuarios

Puede elegir guardar los datos y la configuración de los usuarios activando las capas de usuarios en las plantillas de imagen. Una vez habilitada, se crea una capa de usuarios para cada usuario que tiene acceso a una o más máquinas publicadas mediante la plantilla. No utilizamos las capas de usuarios para el host de la sesión.

Hay dos tipos de capas de usuarios que puede habilitar en una plantilla de imagen: Capas de usuarios completo y capas de usuarios de Office 365.

- **Capas de usuario completo:** habilite las capas de usuario completo para conservar la configuración y los datos de todas las capas asignadas a la máquina, para cada usuario que acceda a la máquina.
- **Capas de usuarios de Office 365:** Las capas de usuarios de Office 365 están optimizadas para MS Outlook. Habilite las capas de usuarios de Office 365 para conservar la configuración y los datos de Office 365, incluido Outlook.

Conectores

Los conectores son el medio para que el dispositivo se comunice con hipervisores individuales o software de Provisioning. Normalmente, necesita dos tipos de configuraciones de conectores:

- **Configuración del conector para crear capas:** permite que el dispositivo acceda a la ubicación del hipervisor en la que instala el software para cada una de las capas.
- **Configuraciones de conector para publicar imágenes en capas:** proporciona al dispositivo las credenciales necesarias para publicar imágenes en capas en su servicio de aprovisionamiento o hipervisor.

Qué crear en su entorno

En esta sección se describen las configuraciones de conectores que necesita y el software que se va a instalar en las capas de sistema operativo y de la plataforma en función de la plataforma de destino.

- [XenServer](#)
- [MS Azure](#)
- [MS Hyper-V](#)
- [Nutanix](#)
- [VMware vSphere](#)

XenServer

Si el dispositivo está instalado en XenServer, utilice configuraciones de conectores para automatizar los procesos de publicación y distribución de capas. Si utiliza un dispositivo que se ejecuta en un hipervisor diferente, utilice el recurso compartido de archivos de red para transferir los archivos.

Si el dispositivo está instalado en XenServer Si el dispositivo está instalado en otro hipervisor y está creando capas o publicando en XenServer, utilice las configuraciones y capas de conectores que se describen en la tabla siguiente.

Capa de sistema operativo en XenServer: Incluya las herramientas de XenServer en la capa de sistema operativo.

Tarea	Utilizar la configuración del conector	Para que el dispositivo acceda a la ubicación de	Incluir en la capa Plataforma
Importar SO	XenServer	Imagen del SO	—
Capas de paquete	XenServer	Máquina de empaquetado	—
Publicar imágenes en capas	Creación de máquinas para XenServer, Citrix Provisioning o XenServer	Aprovisionamiento del sistema	Si utiliza Creación de máquinas para XenServer o Citrix Provisioning, incluya las herramientas respectivas y las herramientas de agente de conexión

Si el dispositivo está instalado en otro hipervisor Si el dispositivo se ejecuta en un hipervisor que no sea Citrix y está creando capas o publicando en XenServer, utilice el recurso compartido de archivos de red del dispositivo y las capas que se describen en la tabla siguiente.

Capa de sistema operativo: se instalan diferentes herramientas de hipervisor en la capa de sistema operativo, pero si establece el tipo de hipervisor de la capa de plataforma en XenServer, las herramientas de la capa de sistema operativo se eliminan y las herramientas que agrega a la capa de plataforma se incluyen en las imágenes en capas que publique.

Tarea	Configuración del conector	Para que el dispositivo acceda a la ubicación de	Capa de plataforma
Importar SO	Recursos compartidos de archivos de red	Imagen del SO	Herramientas de XenServer
Capas de paquete	Recursos compartidos de archivos de red	Máquina de empaquetado	Herramientas de XenServer
Publicar imágenes en capas	Recursos compartidos de archivos de red	Aprovisionamiento del sistema	Herramientas de XenServer, ya sean herramientas de creación de máquinas o de Citrix Provisioning, si corresponde, y herramientas de intermediario de conexiones

Enlaces relacionados

- Conectores:
 - [Creación de máquinas para XenServer](#)
 - [Citrix Provisioning](#)
 - [XenServer](#)
- Detalles de la capa de plataforma:
 - [Crear capa de plataforma](#)
 - [Herramientas de creación de máquinas para XenServer](#)
 - [Herramientas de Citrix Provisioning](#)
 - [Herramientas de XenServer](#)

MS Azure

Si el dispositivo de App Layering está instalado en Azure, puede usar configuraciones de conectores para automatizar los procesos de publicación y creación de capas. De lo contrario, utilizará el recurso compartido de archivos de red del dispositivo para transferir imágenes desde y hacia la plataforma de destino.

Si el dispositivo está instalado en Azure Cuando el dispositivo esté instalado en Azure y esté creando capas en Azure o publicando imágenes en capas en ese hipervisor o en un servicio de aprovisionamiento que se ejecute en él, utilice las configuraciones y capas de conectores que se describen en la tabla siguiente.

Capa de sistema operativo: no se requieren herramientas de hipervisor para Azure

Tarea	Utilizar la configuración del conector	Para que el dispositivo acceda a la ubicación de	Incluir en la capa Plataforma
Importar SO	MS Azure	Imagen del SO	—
Capas de paquete	MS Azure	Máquina de empaquetado	—
Publicar imágenes en capas	Creación de máquinas para Azure, MS Azure	Sistemas cercanos a la provisión	Si es Machine Creation for Azure, incluya herramientas de creación de máquinas

Si el dispositivo está instalado en otro hipervisor Si el dispositivo está instalado en un hipervisor que no sea Azure y está creando capas en Azure o publicando imágenes en capas en Azure o en una creación de máquinas que se ejecute en Azure, utilice el recurso compartido de archivos de red del dispositivo y las capas que se describen en la tabla siguiente.

Capa de SO: aunque las herramientas para el hipervisor incorrecto estén instaladas en la capa del sistema operativo, puede anular las herramientas estableciendo el Tipo de hipervisor en la capa de plataforma en Azure.

Tarea	Configuración del conector	Para que el dispositivo acceda a la ubicación de	Capa de plataforma
Importar SO	Recursos compartidos de archivos de red	Imagen del SO	No se requiere
Capas de paquete	Recursos compartidos de archivos de red	Máquina de empaquetado	No se requiere
Publicar imágenes en capas	Recursos compartidos de archivos de red	Aprovisionamiento del sistema	herramientas de creación de máquinas, si procede

Enlaces relacionados

- Conectores:
 - [Machine Creation for Azure](#)
 - [Machine Creation for Azure Government](#)
 - [MS Azure](#)
- Detalles del software de capa de plataforma:
 - [Herramientas de MS Azure](#)
 - [Herramientas de Machine Creation for Azure o Azure Government](#)

MS Hyper-V

Si el dispositivo de App Layering está instalado en Hyper-V, puede usar configuraciones de conectores para automatizar los procesos de publicación y creación de capas. De lo contrario, utilizará el archivo de archivos del dispositivo para transferir imágenes desde y hacia la plataforma de destino.

Si el dispositivo está instalado en Hyper-V Cuando el dispositivo esté instalado en Hyper-V y esté creando capas en Hyper-V o publicando imágenes en capas en Hyper-V o en un servicio de aprovisionamiento que se ejecute en él, utilice las configuraciones de conectores y capas que se describen en la tabla siguiente.

Capa de SO: incluya la configuración de Hyper-V, si el sistema operativo no se originó en Hyper-V.

Tarea	Utilizar la configuración del conector	Para que el dispositivo acceda a la ubicación de	Incluir en la capa Plataforma
Importar SO	---	Imagen del SO	---
Capas de paquete	MS Hyper-V	Máquina de empaquetado	---
Publicar imágenes en capas	Creación de máquinas, Citrix Provisioning o MS Hyper-V	Aprovisionamiento del sistema	Si Citrix Provisioning, incluya las herramientas de aprovisionamiento y las herramientas del agente de conexión

Si el dispositivo está instalado en otro hipervisor Si el dispositivo está instalado en un hipervisor distinto de Hyper-V y está creando capas o publicando en Hyper-V, utilice el recurso compartido de archivos de red del dispositivo y las capas descritas en la tabla siguiente.

Capa del sistema operativo: las herramientas para un hipervisor diferente están instaladas en la capa del sistema operativo. Elimine los archivos configurando el Tipo de hipervisor en Hyper-V en la capa de plataforma. La configuración de la capa de plataforma anula el hipervisor original.

Tarea	Configuración del conector	Para que el dispositivo acceda a la ubicación de	Capa de plataforma
Importar SO	Recursos compartidos de archivos de red	Imagen del SO	Configuración de MS Hyper-V
Capas de paquete	Recursos compartidos de archivos de red	Máquina de empaquetado	Configuración de MS Hyper-V
Publicar imágenes en capas	Recursos compartidos de archivos de red	Aprovisionamiento del sistema	Configuración de Hyper-V, herramientas de agente de conexión y herramientas de aprovisionamiento, si procede

Enlaces relacionados

- Conectores:
 - [Citrix Provisioning](#)
 - [MS Hyper-V](#)
- Detalles del software de capa de plataforma:
 - [Crear capa de plataforma](#)
 - [Herramientas de Citrix Provisioning](#)
 - [Herramientas MS Hyper-V](#)

Nutanix AHV

Si el dispositivo de App Layering está instalado en Nutanix, puede utilizar configuraciones de conectores para automatizar los procesos de creación de capas y publicación. De lo contrario, se utiliza el recurso compartido de archivos del dispositivo para transferir imágenes desde y hacia la plataforma de destino.

Si el dispositivo está instalado en Nutanix Cuando el dispositivo esté instalado en Nutanix y esté creando capas o publicando imágenes en Nutanix, utilice las configuraciones y capas de conectores que se describen en la tabla siguiente.

Capa de SO: incluye herramientas Nutanix

Tarea	Utilizar la configuración del conector	Para que el dispositivo acceda a la ubicación de	Incluir en la capa Plataforma
Importar SO	Nutanix AHV	Imagen del SO	—
Capas de paquete	Nutanix AHV	Máquina de empaquetado	—
Publicar imágenes en capas	Machine Creation for Nutanix, Machine Creation o Nutanix AHV	Aprovisionamiento del sistema	Si utiliza Machine Creation for Nutanix, incluya herramientas de creación de máquinas

Si el dispositivo está instalado en otro hipervisor Si el dispositivo está instalado en un hipervisor distinto de Nutanix y está creando capas o publicando en Nutanix, utilice el recurso compartido de archivos de red y las capas descritas en la tabla siguiente.

Capa de **SO: aunque en la capa** del sistema operativo hay instaladas herramientas para un hipervisor diferente, puede anularlas y eliminarlas. En la capa de plataforma, establezca el Tipo de hipervisor en Nutanix. A continuación, las herramientas de Nutanix se incluyen en las imágenes en capas.

Tarea	Configuración del conector...	Para que el dispositivo acceda a la ubicación de:	Capa de plataforma
Importar SO	Recursos compartidos de archivos de red	Imagen del SO	Herramientas Nutanix
Capas de paquete	Recurso compartido de archivos Nutanix	Máquina de empaquetado	Herramientas Nutanix
Publicar imágenes en capas	Recurso compartido de archivos Nutanix	Aprovisionamiento del sistema	Herramientas de Nutanix, herramientas de agente de conexión y herramientas de creación de máquinas, si procede

Enlaces relacionados

- Conectores:
 - [Machine Creation for Nutanix AHV](#)
 - [Nutanix AHV](#)
- Detalles del software de capa de plataforma:
 - [Crear capa de plataforma](#)
 - [Herramientas de Machine Creation for Nutanix AHV](#)
 - [Herramientas de Nutanix AHV](#)

VMware vSphere

Si el dispositivo de App Layering está instalado en vSphere, puede utilizar configuraciones de conectores para automatizar los procesos de creación de capas y publicación. De lo contrario, utilizará el archivo de red del dispositivo para transferir imágenes desde y hacia la plataforma de destino.

Si el dispositivo está instalado en vSphere Cuando el dispositivo esté instalado en vSphere y cree capas o publique en vSphere, utilice las siguientes capas y configuraciones de conector.

Capa de SO: incluye herramientas de VMware

Tarea	Utilizar la configuración del conector	Para que el dispositivo acceda a la ubicación de	Incluir en la capa Plataforma
Importar SO	VMware vSphere	Imagen del SO	---
Capas de paquete	VMware vSphere	Máquina de empaquetado	---
Publicar imágenes en capas	Creación de máquinas para vSphere, Citrix Provisioning o VMware vSphere	Aprovisionamiento del sistema	Si se trata de Machine Creation for vSphere o Citrix Provisioning, incluya las herramientas correspondientes y las herramientas del agente de conexiones.

Si el dispositivo está instalado en otro hipervisor Si el dispositivo está instalado en un hipervisor diferente de vSphere, utilice el recurso compartido de archivos de red y las capas descritas en la tabla siguiente.

Capa de SO: Herramientas para el primer hipervisor que instalaste en directo en la capa del sistema operativo. Para anular y eliminarlos, establezca el Tipo de hipervisor en la capa de plataforma en vSphere.

Tarea	Configuración del conector	Para que el dispositivo acceda a la ubicación de	Capa de plataforma
Importar SO	Recursos compartidos de archivos de red	Imagen del SO	Herramientas de VMware
Capas de paquete	Recursos compartidos de archivos de red	Máquina de empaquetado	Herramientas de VMware
Publicar imágenes en capas	Recursos compartidos de archivos de red	Aprovisionamiento del sistema	Herramientas de VMware, herramientas de intermediación de conexiones y creación de máquinas, Citrix Provisioning, si corresponde

Enlaces relacionados

- Conectores:
 - [Machine Creation for vSphere](#)
 - [Citrix Provisioning](#)
 - [VMware vSphere](#)
- Detalles del software de capa de plataforma:
 - [Crear capa de plataforma](#)
 - [Herramientas de Machine Creation for vSphere](#)
 - [Herramientas de Citrix Provisioning](#)
 - [Herramientas de VMware vSphere](#)

Opciones avanzadas para implementar el dispositivo

Solo necesita un dispositivo de App Layering, pero puede instalar más de uno y utilizar cada uno un dispositivo independiente.

Tenga en cuenta los siguientes puntos al decidir cuántos dispositivos usar en su entorno.

- El mantenimiento de un solo dispositivo resulta en menos complejidad y sobrecarga de administración. Considere un segundo dispositivo solo si las velocidades de red son irreparablemente lentas u otros problemas importantes que impidan el uso.
- Puede utilizar varios dispositivos para mantener un entorno de prueba y un entorno de producción.
- Si tiene varias capas de SO y se originaron en diferentes dispositivos, puede tener diferentes administradores para las capas creadas con cada una de ellas.
- Si crea más de un dispositivo, cada uno de ellos será independiente. No actúan como copias de seguridad el uno para el otro.
- Haga una copia de seguridad de cada dispositivo o diseñelo para alta disponibilidad de modo que no pierda capas. Necesita una copia de seguridad completa de cada dispositivo para garantizar que puede recuperar toda la información de él. Aunque puede exportar e importar capas, esta función no está diseñada para la recuperación de errores.

XenServer

May 9, 2024

Para usar App Layering con XenServer, necesita las siguientes cuentas, herramientas e información de recursos.

Cuenta y privilegios

App Layering requiere una cuenta de XenServer nueva o existente para la creación de capas. La cuenta necesita privilegios para:

- Crear y eliminar discos virtuales.
- Copiar y eliminar las capas de los discos virtuales mediante las API de archivos de XenServer.

Software y configuración

Acceso a las herramientas de XenServer para instalar en la capa.

Información sobre recursos

Para obtener más datos acerca de la información de Citrix Hypervisor que necesita, consulte los campos detallados en la [configuración del conector de XenServer](#).

Citrix Provisioning

May 9, 2024

Puede publicar imágenes en capas en Citrix Provisioning que se ejecuten en MS Hyper-V, VMware vSphere, Nutanix AHV Acropolis o XenServer.

Requisitos de software

Al crear una capa de plataforma para Citrix Provisioning, el software siguiente debe estar en una ubicación accesible para la máquina de empaquetado:

- Instalador de Citrix Provisioning.
- Instalador del agente de conexión, si utiliza un agente.

Instale solo herramientas de Hypervisor en la capa de plataforma para anular el hipervisor principal. (El Hypervisor principal se implementa en la capa del sistema operativo).

Para actualizar la capa de plataforma con una nueva versión, solo necesita las actualizaciones de software.

Requisitos previos de Citrix Provisioning

- **Inhabilitar IPv6 en la capa del sistema operativo**

Si IPv6 está habilitado en la capa del sistema operativo, agregue una versión a la capa del sistema operativo e inhabilite IPv6 en ella. Se debe crear una nueva capa de plataforma basada en la nueva versión de capa del sistema operativo.

Importante:

Si inhabilita IPv6 en la capa de plataforma en lugar de en la capa del sistema operativo, las máquinas Citrix Provisioning resultantes pierden la conexión de red y se bloquean al arrancar.

- **Instalar el agente de App Layering en los servidores de Citrix Provisioning**

Instale el agente en los servidores de Citrix Provisioning y dondequiera que el conector esté configurado para ejecutar scripts. Registre cada uno de los agentes con el dispositivo App Layering.

- **Instalar la consola de Citrix Provisioning donde está instalado el agente**

La consola de Citrix Provisioning debe instalarse en todos los servidores de Citrix Provisioning donde esté instalado el agente.

- **Asegúrese de que el software Citrix Provisioning Target Device Imaging esté disponible para instalar**

El software Target Device Imaging debe estar disponible para instalarlo en la capa de plataforma. Utilice la versión que se implementa en el servidor donde está publicando imágenes.

- **Información de recursos de Citrix Provisioning**

La información de Citrix Provisioning que aparece en este tema [Configuración del conector de Citrix Provisioning](#).

- **Instalar el complemento PowerShell**

Instale el complemento PowerShell apropiado.

- **CMID único para cada dispositivo de destino (si utiliza KMS)**

Al utilizar licencias de KMS, Citrix Provisioning requiere que cada dispositivo de destino tenga un CMID único. Para ver la historia completa, consulte este artículo de Citrix, [Desmitificación de KMS y Provisioning Services](#). Rearmar KMS se incluye en los pasos para crear una capa de plataforma.

- **Más opciones de configuración de Citrix Provisioning para usar en su entorno**

Configure Citrix Provisioning en la capa de la plataforma. Asegúrese de que la configuración coincida con el entorno en el que se va a utilizar la imagen en capas.

- **Citrix Provisioning para Hyper-V**

Requiere un adaptador de red heredado para el arranque previo del entorno de ejecución.

Requisitos previos del hipervisor

- **Software y configuración** : acceso al software para instalarlo en la capa.
- **Información de recursos del hipervisor**: La información del hipervisor que aparece en la configuración del conector que está utilizando.

Requisitos previos del agente de conexión

Necesita instaladores, herramientas y configuraciones necesarias para ejecutar el agente de conexión en el hipervisor que está usando.

Herramientas y configuración requeridos

- Configuración de KMS, si utiliza licencias de KMS

Una vez que tengas los requisitos, estarás listo para [crear](#) la capa Platform.

Docker

June 17, 2022

App Layering es compatible con la plataforma Docker. Para implementar Docker en un entorno de App Layering, tenga en cuenta lo siguiente:

- Docker debe estar instalado en la capa del sistema operativo, ya que configura varios componentes de Windows.
- Puedes crear una revisión del sistema operativo para instalar y habilitar Docker.
- Docker permanece inactivo hasta que emites los comandos de Docker. Tener Docker instalado en la revisión no causa problemas en las revisiones posteriores del SO, las máquinas de empaquetado o los escritorios implementados con el SO.
- No coloque ninguna imagen de Docker en la capa del sistema operativo ni en ninguna de las capas de aplicaciones. Los archivos `vhd(x)` que se escriben en el disco cuando se descarga la imagen se deben mover a la capa de escritura del usuario para que se ejecute la imagen. Docker debe abrir los archivos para obtener acceso de lectura y escritura, lo que solo se puede hacer en el volumen del usuario.

Nota:

En una implementación de capa de usuarios completa, el usuario solo necesita descargar la imagen de Docker una vez. La imagen persiste durante las sesiones de cierre de sesión e inicio de sesión.

- Docker requiere un hipervisor que admita hipervisores anidados. El hipervisor de destino que aloja los escritorios VDI implementados debe admitir hipervisores anidados para que, cuando un usuario inicie sesión en la máquina, pueda descargar y ejecutar imágenes de Docker.

Importante:

La ubicación de almacenamiento de la capa del usuario no importa para esta restricción. Solo la máquina de VDI implementada que monta la capa del usuario es necesaria para ejecutarse en un hipervisor que permita hipervisores anidados.

- Las imágenes de Docker pueden ser grandes. El tamaño de las capas de usuarios debe establecerse en un tamaño mayor para que se adapten a las imágenes cuando se descargan. Recomendamos configurar capas de usuarios en 100 GB después de nuestras pruebas.

Nota:

Las capas de usuarios son discos dinámicos, por lo que el tamaño real del disco no será de tamaño completo. Cuando se utiliza el espacio en disco, no volverá a ser escaso, por lo que la ubicación de almacenamiento de los volúmenes del usuario necesita suficiente espacio en disco para adaptarse al tamaño completo de las capas del usuario a lo largo del tiempo.

Cloud de Google

June 30, 2021

En este artículo se describen los recursos que necesitas para crear capas y publicar imágenes en Google Cloud.

Para crear capas para Google Cloud, necesitas una configuración del conector de Google Cloud. Según el entorno, es posible que también necesite una capa de plataforma.

Si planeas publicar imágenes en Machine Creation en Google Cloud, usa el [Creación de máquinas para la configuración del conector de Google Cloud](#).

Configuración del conector de Google Cloud

Para crear capas y publicar imágenes en Google Cloud necesitas los recursos necesarios para:

- [Instalar el dispositivo de App Layering](#)
- [Creación de configuraciones de conectores](#)

Proyecto Google Cloud

Para implementar el dispositivo, necesita las credenciales de administrador del proyecto.

Almacenamiento de Google Cloud

La configuración del conector de Google Cloud requiere una o más ubicaciones de almacenamiento para:

- Los discos de máquina virtual que se utilizan para crear capas y publicar imágenes en capas.
- El archivo de plantilla que usas para implementar tus máquinas virtuales de Google Cloud y los archivos de diagnóstico de arranque de esas máquinas virtuales.

Capa de SO

Si planea utilizar una imagen de sistema operativo creada en otra plataforma, asegúrese de prepararse para:

- Exporte la capa de SO desde el dispositivo App Layering que se ejecuta en otra plataforma.
- Importe la capa de SO mediante el dispositivo App Layering que se ejecuta en Google Cloud.
- Añade una versión a la capa de SO importada para prepararla para que se ejecute en Google Cloud.

Capa de plataforma

Para crear capas o publicar imágenes en capas en Google Cloud, solo necesita una capa de plataforma cuando publica imágenes en un servicio de aprovisionamiento, como la creación de máquinas Citrix.

Cuando creas una capa de plataforma, no es necesario instalar herramientas de Google Cloud en ella. Cuando las herramientas de Google Cloud no están presentes, Google Cloud las instala en la máquina de empaquetado cuando se inicia la máquina.

Cuando crea una capa de plataforma, cualquier instalador de software que necesite (por ejemplo, el software de Provisioning Service) debe estar accesible desde la máquina de empaquetado.

Machine Creation for Azure o Azure Government

November 5, 2020

Los instaladores de software deben estar disponibles en una ubicación accesible para la máquina de empaquetado en la que está creando una capa.

Requisitos previos de creación de máquinas

Al crear una capa de plataforma para publicar imágenes, necesita:

- **Instalador de Citrix Virtual Delivery Agent (VDA) para Windows**

- **Citrix Desktop Delivery Controller (DDC)**

Instale el software Citrix DDC en el servidor donde se publican las imágenes en capas. Si incluye un script para ejecutarse en las imágenes en capas, necesita lo siguiente:

- **Agente:** Implemente el agente en el DDC, lo que permite al dispositivo ejecutar el script allí.
- **Complemento de PowerShell:** Se debe instalar el complemento apropiado de PowerShell en el DDC.

- **Información de recursos de Citrix**

La información de Citrix que aparece en la configuración de [Machine Creation for Azure Connector](#).

Creación de máquinas para XenServer

May 9, 2024

Para publicar imágenes en la creación de máquinas que se ejecutan en XenServer, necesita una capa de plataforma para ese fin. Para crear la capa de plataforma requerida, necesita:

- [Una capa de SO](#)
- **Acceso de red a las herramientas de App Layering**

Acceso desde la máquina virtual de la máquina de empaquetado de capa de plataforma a las máquinas herramientas del sistema operativo (en el paquete de descarga de instalación).

- **Citrix Virtual Delivery Agent (VDA) instalado en la capa de plataforma**

Instale el instalador de Citrix VDA para el sistema operativo Windows que está utilizando en la capa de plataforma.

- **Citrix Delivery Controller**

Instale el software Citrix Delivery Controller en el servidor donde publica la imagen en capas.

Como parte de la configuración del conector, si incluye un script para ejecutarse en la imagen en capas recién publicada, necesitará lo siguiente:

- **Agente:** Instalado y en ejecución en el Delivery Controller, lo que permite al dispositivo ejecutar el script en el Delivery Controller.
- **Complemento de PowerShell:** Instale el complemento de PowerShell correspondiente en el Delivery Controller.

- **Información de recursos de Citrix**

La información de Citrix que aparece en el tema [Creación de máquinas para la configuración del conector de XenServer](#).

Creación de máquinas para Google Cloud

January 9, 2022

En este artículo se describen los recursos necesarios para publicar imágenes en la creación de máquinas para Google Cloud.

Para publicar imágenes en este entorno, necesita una configuración del conector de creación de máquinas para Google Cloud] (</es-es/citrix-app-layering/4/connect/machine-creation-for-google-cloud.html>). Según el entorno, es posible que también necesite una capa de plataforma.

Creación de máquinas para configuración del conector de Google Cloud

Para publicar imágenes en Machine Creation for Google Cloud, necesitas los recursos necesarios para:

- [Instalar el dispositivo de App Layering](#)
- [Creación de configuraciones de conectores](#)

Proyecto Google Cloud

La creación de máquinas para la configuración del conector de Google Cloud requiere una o más ubicaciones de almacenamiento para:

- Los discos de máquina virtual que se utilizan para crear capas y publicar imágenes en capas.
- El archivo de plantilla utilizado para implementar máquinas virtuales de Azure y los archivos de diagnóstico de arranque para esas máquinas virtuales.

Almacenamiento de Google Cloud

La configuración del conector de Azure requiere una o varias ubicaciones de almacenamiento para:

- Los discos de máquina virtual que se utilizan para crear capas y publicar imágenes en capas.
- El archivo de plantilla utilizado para implementar máquinas virtuales de Azure y los archivos de diagnóstico de arranque para esas máquinas virtuales.

Capa de SO

Si planea utilizar una imagen de sistema operativo creada en otra plataforma, prepárese para:

- Exporte la capa de SO desde el dispositivo App Layering que se ejecuta en otra plataforma.
- Importe la capa de SO mediante el dispositivo App Layering en Google Cloud.
- Añade una versión a la capa de SO importada para prepararla para que se ejecute en Google Cloud.

Capa de plataforma

Necesita una capa de plataforma al publicar en una plataforma de aprovisionamiento, como la creación de máquinas Citrix o en otro hipervisor.

Cuando crea una capa de plataforma, los instaladores de software de creación de máquinas deben estar accesibles desde la máquina de empaquetado para poder instalarlos en la capa.

Machine Creation for Hyper-V

November 5, 2020

Para publicar imágenes en la creación de máquinas en Hyper-V, necesita una capa de plataforma. La capa de plataforma garantiza que las aplicaciones se instalen y ejecuten sin problemas en su entorno de publicación.

Para crear su capa de plataforma, necesita:

- [Una capa de SO](#)
- **Acceso de red a las herramientas de App Layering:** acceso desde la máquina de empaquetado de capas de plataforma a las máquinas herramientas del sistema operativo. Las herramientas se incluyen en la descarga de instalación.
- **Información de recursos de Hyper-V:** la información que se muestra en el tema [Creación de equipos para la configuración del conector de hyper-v](#).

Machine Creation for Nutanix AHV

November 5, 2020

Haga que los instaladores de software del siguiente software sean accesibles para la máquina de empaquetado en la que está creando la capa.

- Nutanix AHV
- Creación de máquinas
- Su agente de conexión (si corresponde)

Requisitos previos de creación de máquinas

Al crear una capa de plataforma para publicar imágenes en Machine Creation, necesita:

- **Una capa de SO**
- **Instalador de Citrix Virtual Delivery Agent (VDA) para su sistema operativo Windows**

El instalador de Citrix VDA para el sistema operativo Windows que está mediante debe estar instalado en la capa de plataforma.

- **Citrix Desktop Delivery Controller (DDC)**

El software Citrix DDC debe instalarse en el servidor donde se publican las imágenes en capas.

- **Información de recursos de Citrix**

La información de Citrix que aparece en este [tema Configuración del conector de creación de máquinas](#).

Requisitos previos del AHV de Nutanix

Haga que los instaladores de software del hipervisor sean accesibles para la máquina de empaque en la que cree capas.

Si está publicando en CitriProvisioning Service o mediante un agente de conexión, las herramientas de esos servicios también deben estar accesibles para la máquina de empaquetado.

Cuenta y privilegios de Nutanix Prism

- Una cuenta de Nutanix Prism (nueva o existente) para usar en App Layering.
- La cuenta debe tener privilegios para realizar las siguientes operaciones:
 - Operaciones de VM:
 - * clonar
 - * eliminar
 - * encender/apagar

- * adjuntar discos virtuales
- Operaciones de imagen:
 - * create
 - * actualizar (también conocido como cargar)
 - * eliminar
- Discos virtuales
 - * create
 - * conectar con máquinas virtuales

Configuración y software de Nutanix AHV

- Acceso a las herramientas de movilidad de VM para instalar en la capa.

Información de recursos de Nutanix AHV

- La información del servidor Acropolis que aparece en [Configuración del conector de Nutanix AHV](#) o [Creación de máquina para la configuración del conector de Nutanix AHV](#).

Conector AHV de Nutanix

- Al crear capas para el entorno de Nutanix, debe utilizar una configuración de conector de Nutanix AHV. El conector de Machine Creation for Nutanix AHV no admite la creación de capas.

Requisitos previos del agente de conexión

Necesita instaladores, herramientas y configuraciones necesarias para ejecutar el agente de conexión en el hipervisor que está mediante.

Herramientas y configuración requeridos

- Configuración de KMS, si utiliza licencias de KMS

Machine Creation for vSphere

November 5, 2020

En este artículo se explican las consideraciones y los requisitos a la hora de publicar imágenes en capas en la creación de máquinas y crear las capas en vSphere.

Capa de plataforma

Necesita una capa de plataforma para publicar imágenes en la creación de máquinas que se ejecutan en vSphere.

- Si ha estado utilizando máquinas BIOS y quiere comenzar a usar máquinas UEFI, se requiere una nueva versión de la capa de plataforma.
- Si quiere publicar imágenes en una nueva ubicación en vSphere, se recomienda crear una capa de plataforma específica para la nueva ubicación.

Requisitos de capa de plataforma

Al publicar imágenes en un entorno de Horizon View, necesita los siguientes recursos para crear la capa de plataforma:

- **Una capa de SO**
- **Información de recursos y software de creación de máquinas:** prepare la información de creación de máquinas que aparece en esta creación de [máquinas para el](#) tema del conector de vSphere.
- **Información de recursos de vSphere:** información de vSphere que aparece en la configuración del conector de [vSphere](#).
- **Su software de agente de conexión**

Cuándo instalar las herramientas de VMware vSphere en la capa de plataforma

Si el sistema operativo se creó en un Hypervisor distinto de vSphere, instale el software VMware vSphere en la capa de plataforma. Además, instale el agente de App Layering y las máquinas herramientas del sistema operativo. Necesita:

- **Acceso al instalador del software del hipervisor de VMware**
- **Agente de App Layering y complemento PowerShell, si utiliza un script como parte de la configuración del conector:** si incluye un script para ejecutarse en imágenes en capas, asegúrese de que el agente de [App Layering](#) y el complemento PowerShell se están ejecutando.

Conectores

Necesita estas configuraciones de conectores para crear capas y publicar imágenes en capas en la creación de máquinas:

- **Creación de máquinas para la configuración del conector de vSphere:** proporciona al dispositivo las credenciales que necesita para publicar en una ubicación de creación de máquinas.
- **Configuración del conector de VMware vSphere:** proporciona al dispositivo las credenciales para crear capas y publicar imágenes en una ubicación específica de vSphere.

Máquinas UEFI

En esta sección se explica cómo cambiar del uso de máquinas BIOS a máquinas UEFI.

Para configurar UEFI, seleccione una plantilla de máquina virtual configurada por UEFI en el servidor vCenter. Las máquinas EFI y VMware Cloud requieren la plantilla. De lo contrario, es opcional. Seleccione la plantilla que quiere utilizar para la capa de plataforma.

Para comenzar a usar UEFI si sus equipos existentes son BIOS

Para comenzar a usar máquinas UEFI en Machine Creation cuando las máquinas existentes son BIOS:

1. Cree una creación de máquinas en la configuración del conector de vSphere con la **función de composición de descarga** habilitada.
2. Seleccione una plantilla de máquina virtual con UEFI configurado.
3. Cree una capa de plataforma o agregue una versión a una existente. Seleccione la configuración del conector que tiene UEFI habilitado.
4. Publique imágenes UEFI mediante esta capa de plataforma y seleccione una configuración de conector que tenga UEFI habilitado.

Puede publicar imágenes mediante la nueva capa de plataforma habilitada para UEFI y la nueva configuración del conector con el SO y las capas de aplicaciones existentes.

Puede seguir revisando las capas del sistema operativo y de la aplicación mediante una configuración del conector del BIOS.

Para comenzar a usar UEFI en una implementación nueva

La **función** Crear capa de SO admite máquinas UEFI. También puede agregar compatibilidad con UEFI a una capa de SO existente. Utilice una configuración de conector con **Composición de descarga** y **UEFI** habilitados.

1. Cree una configuración de conector de VMware vSphere con ****UEFI** y la composición de descarga** habilitada.
2. En la configuración del conector, seleccione una plantilla de máquina virtual con UEFI configurado.
3. Cree capas de aplicaciones habilitadas para UEFI mediante la misma configuración del conector de VMware vSphere.
4. Cree y publique imágenes mediante una plantilla de imagen con las siguientes opciones seleccionadas:
 - Su capa de SO habilitada para UEFI.
 - Una capa de plataforma con Machine Creation instalada.
 - Configuración del conector de Machine Creation for vSphere habilitada para UEFI.
 - Las capas de la aplicación.

MS Azure o Azure Government

June 27, 2024

Al crear capas para un entorno de Azure, debe usar una configuración de conector de MS Azure. Si quiere un entorno de Azure Government, utilice la configuración del conector de Azure Government. En algunos casos, es posible que también necesite una capa de plataforma.

En este artículo se describen los requisitos, incluidos los recursos necesarios para crear una de estas configuraciones de conectores.

Configuración del conector Azure o Azure Government

Los siguientes recursos son necesarios para la configuración del conector.

Cuenta y suscripción de Azure

Para implementar el dispositivo, necesita las credenciales de administrador para su suscripción a Azure. Para obtener más información, consulte la página Inicio de sesión [de Microsoft Azure](#).

Azure Resource Manager

App Layering admite el modelo de administración de recursos (ARM) de Azure. No puede usar el modelo de implementación clásico de Azure. Todos los recursos para App Layering se deben crear medi-

ante Azure Resource Manager. Para obtener más información, consulte la página de introducción del [Azure Resource Manager](#).

Almacenamiento de Azure

La configuración del conector de Azure requiere una o más cuentas de almacenamiento para:

- Los discos de máquina virtual que se utilizan para crear capas y publicar imágenes en capas.
- El archivo de plantilla utilizado para implementar máquinas virtuales de Azure y los archivos de diagnóstico de arranque para esas máquinas virtuales.

Para obtener más información sobre el almacenamiento necesario, consulte Configuración del conector de [MS Azure](#).

Capa de plataforma

Siempre y cuando la imagen que usa para la capa del sistema operativo sea de Azure, *no* necesita una capa de plataforma para crear capas o publicar imágenes en capas en Azure. Solo necesita una capa de plataforma cuando se publica en un entorno diferente, por ejemplo, en un servicio de aprovisionamiento u otro hipervisor.

Al publicar en Azure mediante una imagen del sistema operativo que se originó en un hipervisor diferente, necesita una capa de plataforma para asegurarse de que las imágenes en capas funcionen correctamente en Azure.

Cuando crea una capa de plataforma, no es necesario instalar herramientas de Azure en ella. Cuando las herramientas de Azure no están presentes, Azure las instala en la máquina de empaquetado cuando se inicia la máquina.

Cuando crea una capa de plataforma, todos los instaladores de software que necesite (por ejemplo, el software de servicio de aprovisionamiento) deben ser accesibles desde la máquina de empaquetado.

MS Hyper-V

April 8, 2021

En esta sección se describen consideraciones y requisitos al crear capas o publicar imágenes en Hyper-V.

Capa de plataforma

Configure los parámetros de **Hyper-V** en la capa de plataforma para que las demás aplicaciones en capas se ejecuten sin problemas en Hyper-V.

Necesita una capa de plataforma si la imagen del SO utilizada para crear la capa del SO se originó en un hipervisor diferente. Si la imagen del sistema operativo se originó en Hyper-V, *no* necesita una capa de plataforma. La configuración de **Hyper-V** ya está configurada en la capa del sistema operativo.

También necesita una capa de plataforma si comienza a utilizar máquinas de generación 2, como se explica en la siguiente sección.

Máquinas de generación 2

Para empezar a utilizar máquinas de generación 2 en Hyper-V cuando las máquinas existentes son de generación 1:

- Cree una configuración de conector Hyper-V con la función de **composición de descarga** activada y Generación 2 seleccionada.
- Cree una capa de plataforma de generación 2.
- Publique imágenes de Generación 2 con esta capa de plataforma y las capas de aplicaciones de Generación 1 existentes.

Si va a comenzar con una implementación nueva en Hyper-V, puede crear una capa de SO de generación 2 mediante cualquiera de los siguientes enfoques:

- Cree la capa del sistema operativo a partir de una imagen de SO de generación 1. A continuación:
 - Cree una configuración de conector Hyper-V con la función de **composición de descarga** activada y **Generación 2** seleccionada.
 - Agregue una versión de generación 2 a la capa del sistema operativo.
 - Crear capas de aplicaciones de generación 2.
 - Cree una plantilla de imagen con el nuevo conector seleccionado y publique las imágenes.
- Cree la capa del sistema operativo a partir de una imagen de SO Generación 2, omitiendo la consola de administración y utilizando el [Script de importación del SO](#):
 - Busque el script ImportOSLayer.ps1 incluido en la descarga de herramientas de SO.
 - Importe el sistema operativo mediante el script. El script admite la importación de máquinas UEFI y completa la importación más rápido que la consola de administración.

Nutanix AHV

November 5, 2020

Al crear una capa de plataforma, los instaladores de software para el hipervisor deben estar disponibles en una ubicación accesible para la máquina de empaquetado en la que está creando la capa. Si está publicando en un servicio de aprovisionamiento o mediante un agente de conexión, también debe tener acceso a las herramientas de esos servicios desde la máquina de empaquetado.

Requisitos previos de Nutanix AHV (Acropolis)

- **Cuenta y privilegios de Nutanix Prism**

- Una cuenta de Nutanix Prism (nueva o existente) para usar en App Layering.
- La cuenta debe tener privilegios para realizar las siguientes operaciones:
 - * Operaciones de VM:
 - clonar
 - eliminar
 - encender/apagar
 - adjuntar discos virtuales
 - * Operaciones de imagen:
 - create
 - actualizar (también conocido como cargar)
 - eliminar
 - * Discos virtuales
 - create
 - conectar con máquinas virtuales

- **Configuración y software de Nutanix AHV**

Acceso a las herramientas de movilidad de VM para instalar en la capa.

- **Información de recursos de Nutanix AHV**

La información del servidor Acropolis que aparece en [Configuración del conector de Nutanix AHV](#) o [Creación de máquina para la configuración del conector de Nutanix AHV](#).

- **Conector AHV de Nutanix**

Al crear capas para el entorno de Nutanix, debe utilizar una configuración de conector de Nutanix AHV. El conector de Machine Creation for Nutanix AHV no admite la creación de capas.

Requisitos previos del agente de conexión

Necesita instaladores, herramientas y configuraciones necesarias para ejecutar el agente de conexión en el hipervisor que está mediante.

VMware vSphere

November 5, 2020

En esta sección se describen consideraciones y requisitos al crear capas o publicar imágenes en vSphere.

Capa de plataforma

Se requiere una capa de plataforma para crear capas o publicar imágenes en vSphere SOLO en los siguientes casos:

- El sistema operativo de la capa de SO se originó en un hipervisor diferente. Si el sistema operativo se originó en vSphere, *no* necesita una capa de plataforma, ya que la configuración de vSphere ya está configurada en la capa del sistema operativo.
- Si ha estado mediante máquinas BIOS y quiere comenzar a usar máquinas UEFI, se requiere una nueva versión de la capa de plataforma.
- Si quiere publicar imágenes en una nueva ubicación en vSphere, le recomendamos que cree una capa de plataforma específica para cada ubicación.

Requisitos de capa de plataforma

Al publicar imágenes en la creación de máquinas en vSphere, necesita los siguientes recursos para crear la capa de plataforma:

- **Una capa de SO**
- **Creación de máquinas para información de recursos de vSphere:** la información de creación de máquinas que aparece en este [tema de configuración de creación de máquinas](#) para el conector de vSphere.
- **Información de recursos de vSphere: información** de vSphere que aparece en la configuración del conector de [vSphere](#).
- Acceso al software de creación de máquinas para instalarlo en la capa.

Cuándo instalar las herramientas de VMware vSphere en la capa de plataforma

Si el sistema operativo se creó en un hipervisor diferente de vSphere, instale el software VMware vSphere en la capa de plataforma, junto con las herramientas de App Layering de aplicaciones y el Agente de App Layering (si el agente es necesario). Necesita:

- **Acceso al instalador de software de VMware vSphere**
- **Agente de App Layering y complemento PowerShell, si utiliza un script como parte de la configuración del conector:** como parte de la configuración del conector, si incluye un script para ejecutarse en la imagen en capas recién publicada, necesita el agente de [App Layering](#) y PowerShell Snap-in instalado y en ejecución.

Máquinas UEFI

Para empezar a utilizar máquinas UEFI en vSphere cuando los equipos existentes son BIOS:

- Cree una nueva configuración de conector de VMware vSphere con la **función** **decomposición** de descarga habilitada y UEFI seleccionada.
- Cree una capa de plataforma UEFI.
- Publique imágenes UEFI mediante esta capa de plataforma y las capas de aplicaciones de BIOS existentes.

Si va a comenzar con una implementación nueva en vSphere:

- Cree su capa de SO a partir de una imagen de BIOS OS.

Nota:

La **función** Crear capa de SO aún no admite máquinas UEFI. Sin embargo, puede agregar una versión a la capa del sistema operativo con la **composición de descarga** y **UEFI** seleccionados, como se describe en el siguiente paso.

- Cree una configuración de conector de VMware vSphere con la **función** **decomposición** de descarga habilitada y **UEFI** seleccionada.
- Agregue una versión de UEFI a la capa del sistema operativo.
- Crear capas de aplicaciones UEFI.
- Cree una plantilla de imagen con el nuevo conector seleccionado y publique las imágenes.

Recursos compartidos de archivos de red (otras plataformas)

May 9, 2024

Al crear una capa de plataforma, comience por seleccionar el recurso compartido de archivos de red (NFS) o el recurso compartido de archivos de Windows en lugar de una configuración de conector. A continuación, copie el disco del sistema operativo de la capa en el hipervisor donde quiere crear las capas o publicar las imágenes en capas. Conecte el disco del sistema operativo a una máquina de empaquetado e implemente, instale el software, apague la máquina de empaquetado y vuelva a copiar el disco en el recurso compartido de archivos de red del dispositivo para importarlo a la nueva capa de plataforma.

Requisitos previos

- Al crear una capa de plataforma para empaquetar capas, necesita el software y la configuración del hipervisor donde está creando las capas.
- Al crear una capa de plataforma para publicar imágenes en capas, necesita los requisitos previos del hipervisor, además de los requisitos previos para cualquier agente de Provisioning Services y de conexiones que planea ejecutar en el entorno.

Instalar el dispositivo

May 9, 2024

Los artículos de esta sección explican cómo implementar el servicio App Layering.

En primer lugar, debe instalar e implementar el dispositivo App Layering, que funciona con la tecnología Enterprise Layer Manager (ELM).

Una vez instalado, puede configurar la zona horaria, los servidores NTP y la configuración de red.

Finalmente, si necesita el agente App Layering, instálelo en los servidores donde sea necesario.

Para obtener más información sobre la instalación, seleccione su hipervisor:

- [XenServer](#)
- [Google Cloud](#)
- [MS Azure](#)
- [MS Hyper-V](#)
- [Nutanix AHV](#)

- [VMware vSphere](#)

Una vez instalado el dispositivo, puede finalizar la configuración de App Layering mediante los pasos proporcionados e instalar el agente App Layering.

- [Instalar el agente de App Layering](#)

Con el software instalado, puede crear su capa de SO, un requisito previo para la colocación en capas de sus aplicaciones.

XenServer

May 9, 2024

Para instalar el servicio App Layering, implemente el dispositivo en una máquina virtual en XenServer. Si el dispositivo requiere una dirección IP estática, debe configurarla mediante la utilidad de configuración del dispositivo. En la última sección se describen los pasos siguientes.

Requisitos

Para empezar a instalar App Layering, necesita lo siguiente:

- [Una versión compatible de XenServer](#)

- Almacenamiento

- **Cuenta y privilegios de XenServer**

Una cuenta de XenServer para usar en el servicio App Layering.

La cuenta debe tener privilegios de XenServer para:

- Crear y eliminar discos virtuales.
- Copiar y eliminar las capas de los discos virtuales mediante las API de archivos de XenServer.

- **Software y configuración de XenServer**

Acceso a las herramientas de XenServer para instalarlas en la capa.

- **Información de recursos de XenServer**

La información de XenServer aparece en [Configuración del conector de XenServer](#).

Descargar el paquete de instalación

Descargue el paquete de instalación, citrix_app_layering_citrix-hypervisor_4.x.x, del [sitio de descargas de Citrix](#). El archivo zip incluye:

Archivo	Descripción
XenServer_x.x.x.ova	Archivo OVA para la máquina virtual del dispositivo
citrix_app_layering_agent_installer.exe	Instalador del Agente App Layering
citrix_app_layering_os_machine_tools.exe	Herramientas de máquina de SO

Implementar el dispositivo de App Layering

Para implementar el dispositivo:

1. Descargue el archivo zip de instalación citrix_app_layering_XenServer_4.x.zip
2. Extraiga el archivo XenServer_elm_4.x.x.x.ova a una carpeta de la unidad local.
3. En el cliente XenCenter, seleccione **Archivo > Importar**.
4. En el asistente que se abre, seleccione los siguientes valores:
 - **Importar origen:** Busque el origen de la unidad local.
 - **Ubicación:** Elija el XenServer en el que quiere implementar el dispositivo.
 - **Almacenamiento:** Utilice el valor predeterminado para colocar discos de almacenamiento en el Almacenamiento local de XenServer.
 - **Redes:** Seleccione la red correcta para la configuración de XenServer.
 - **Seguridad:** Esta ficha no está disponible. Haga clic en **Siguiente**.
 - **Configuración de la corrección del sistema operativo:** Seleccione **No usar la corrección del sistema operativo**.
 - **Transferir la configuración de VM:** Elija la red correcta y elija **DHCP**.
 - **Finalizar:** Revise la configuración y, a continuación, haga clic en **Finalizar**.
5. Cambie a la **vista de notificaciones** y espere a que se complete la implementación. El proceso puede tardar entre 20 y 35 minutos.
6. Cambie a la vista **Infraestructura**.
7. Seleccione el nuevo dispositivo, que tiene el nombre:
Citrix Enterprise Layer Manager.
8. Haga clic en **Propiedades** e introduzca un nombre y una descripción nuevos para el nuevo dispositivo. La nueva máquina virtual tiene 8 GB de memoria y 4 CPU. Tome nota de la dirección IP asignada en la ficha Redes.
9. Inicie Internet Explorer, escriba la dirección IP del nuevo dispositivo en la barra de direcciones e inicie sesión como “administrador” con la contraseña “Unidesk1”.

La primera vez que inicie sesión en el dispositivo, tendrá que cambiar las contraseñas de administrador de App Layering. Para obtener más información, consulte [Cambiar contraseñas administrativas](#).

Asegúrese de instalar el Agente App Layering, si su entorno lo requiere. Consulte la sección siguiente para obtener más información.

Si quiere que el dispositivo utilice una dirección IP estática

Puede cambiar la dirección IP del dispositivo y/o sus servidores DNS. Cuando el dispositivo se implementa por primera vez, la configuración de DNS se obtiene a través de DHCP. Si DHCP no está disponible y utiliza direcciones IP estáticas, una vez que seleccione **Estática**, se le pedirá que introduzca las **direcciones IP** de los servidores DNS.

1. Inicie sesión en la utilidad de configuración del equipo. Con la consola del hipervisor o SSH, inicie sesión en el dispositivo como administrador.
La primera vez que inicie sesión, use la contraseña predeterminada, Unidesk1.
2. En la solicitud de acción, escriba C (para Configurar red) y presione Retorno.
3. En el siguiente mensaje, escriba D para Dynamic (DHCP) o S para Static.
Si elige **Estática**, se le solicitará la dirección IP y la máscara de subred, junto con las direcciones predeterminadas para las direcciones de puerta de enlace y DNS.
4. Cuando se le solicite, escriba Y para guardar la configuración.
5. En la solicitud de acción, escriba Q para salir.
6. Reinicie el dispositivo.

Siguientes pasos

Una vez instalado el dispositivo y la dirección IP está configurada correctamente, debe:

- [Instalar el agente de App Layering](#)
- [Configurar el servicio App Layering](#)

Cloud de Google

June 30, 2021

Para instalar el servicio App Layering en Google Cloud, despliega el dispositivo en una máquina virtual de Google Cloud. Puede configurar un [dirección IP estática](#), si lo necesita, mediante la utilidad de configuración del dispositivo.

Configuración del proyecto de Google Cloud

Configura un proyecto de Google Cloud.

Habilitar API

Habilite las siguientes API de Citrix Cloud:

- API de Compute Engine
- API de almacenamiento en la nube
- API de Cloud Resource Manager
- API de Identity and Access Management (IAM)
- API de Cloud Build

Consulte las instrucciones de Citrix Virtual Apps and Desktops para [habilitar las API de Google Cloud](#).

Crear una cuenta de servicio

La cuenta de servicio necesita los tres roles siguientes:

- Usuario de cuenta de servicio
- Administrador de procesos
- Administrador de almacenamiento

Para obtener más detalles, consulte [Crear una cuenta de servicio](#).

Nota:

La cuenta de App Layering no necesita todos los roles y permisos descritos en el artículo anterior.

Abra los puertos de firewall necesarios

Abra el [puertos de firewall para Google Cloud](#) para que el dispositivo pueda comunicarse con Google Cloud.

Requisitos y configuración de la máquina virtual

Asegúrese de que la máquina virtual en la que instala el dispositivo en Google Cloud esté conectada a una red virtual de Google Cloud.

La máquina virtual que utilice para el dispositivo debe configurarse de la siguiente manera:

Nombre	Valor
Nombre de máquina virtual	Dispositivo de App Layering (Enterprise Layer Manager)
Generación de máquinas virtuales	Generación 1
Memoria	8192 MB
CPU	4
Disco de arranque	sistema unidesk_gcp
Disco adicional	repositorio unidesk_gcp-

Descargue el paquete de instalación

Descargue el paquete de instalación, `citrix_app_layering_gcp_x.x`, desde [sitio de descargas de Citrix](#). El archivo zip incluye:

Archivo	Descripción
<code>unidesk_gcp-system.tar.gz</code> que es	Tarball que contiene disco del sistema para la máquina virtual del dispositivo
<code>citrix_app_layering_agent_installer.exe</code> que es	Instalador del agente App Layering
<code>citrix_app_layering_os_machine_tools.exe</code> que es	Máquinas herramientas de SO

Subir el disco del sistema a Google Cloud

1. Extraiga el paquete de descarga, **`citrix_app_layering_gcp_x.x.zip`**.
2. En el menú **Navegación** en la parte superior izquierda de la IU de Google Cloud, ve a la sección **STORAGE** y selecciona **Almacenamiento > Navegador**. Puede crear un nuevo depósito o añadir una carpeta personal a un depósito existente.
3. Seleccione el enlace del bucket **upload-disks** para cargar el disco.

4. Seleccione el enlace **CARGAR ARCHIVOS** y navegue hasta el directorio en el que extrajo el archivo **unidesk_gcp-system.tar.gz** .
elm-upload-bucket

Buckets > elm-upload-bucket

OBJECTS CONFIGURATION PERMISSIONS RETENTION LIFECYCLE

UPLOAD FILES UPLOAD FOLDER CREATE FOLDER MANAGE HOLDS DOWNLOAD DELETE

Filter by name prefix only Filter Filter objects and folders

<input type="checkbox"/>	Name	Size	Type	Created time ?	Storage class	La
No rows to display						

5. Seleccione **unidesk_gcp-system.tar.gz** y haga clic en el botón **Abrir** . Consulta el mensaje de estado en la parte inferior derecha de la ventana para realizar un seguimiento del progreso de la subida.

Buckets > elm-upload-bucket

OBJECTS CONFIGURATION PERMISSIONS RETENTION LIFECYCLE

UPLOAD FILES UPLOAD FOLDER CREATE FOLDER MANAGE HOLDS DOWNLOAD DELETE

Filter by name prefix only Filter Filter objects and folders

<input type="checkbox"/>	Name	Size	Type	Created time ?	Storage class
<input type="checkbox"/>	unidesk_gcp-system.tar.gz	4.1 GB	application/x-gzip	Feb 10, 2021, 9:16:24 PM	Standard

Creación de una imagen para el disco del sistema

1. Selecciona el menú **Navegación** en la parte superior izquierda de la ventana de Google Cloud, ve a la sección **STORAGE** y selecciona **Compute Engine > Imágenes**.
2. Selecciona **[+] CREAR IMAGEN**.
3. En el campo Nombre, introduzca un nombre permanente para la imagen. Google Cloud advierte de que el nombre es permanente.
4. En Origen, selecciona **Archivo de Cloud Storage**.
5. En **Archivo de Cloud Storage**, utilice el botón **Examinar** para seleccionar el archivo **unidesk_gcp-system.tar.gz** .
6. En **Ubicación**, seleccione **Multiregional** o **Regional** y Ubicación.

7. Seleccione **Create**. La página **Imágenes** hace un seguimiento de la creación de imágenes a medida que avanza. Aparece una marca de verificación verde cuando se crea la imagen. Si la creación falla, el nombre de la imagen ya no aparece en la pantalla Imágenes.

Creación de una instancia de VM

A continuación, cree una instancia de VM, adjunte el disco del sistema y cree discos de repositorio:

1. Seleccione el menú **Navegación** en la parte superior izquierda de la ventana de Google Cloud, ve a la sección **COMPUTE** y seleccione **Compute Engine > Instancias de VM**.
2. Seleccione **[+] CREAR INSTANCIA**.
3. Introduzca datos y elija la configuración de región y máquina deseada.
4. Expanda la sección **Plataforma de CPU y GPU** y marque **Activar dispositivo de visualización**.
5. En la sección **Disco de arranque**, seleccione el botón **Cambiar**. Se abre la ventana Disco de arranque.

Boot disk

Select an image or snapshot to create a boot disk; or attach an existing disk. Can't find ?

Public images Custom images Snapshots Existing disks

Show images from

Show deprecated images

Image

image-[blurred]-gcp-system

Created on Oct 20, 2020, 11:19:41 PM

Boot disk type [?] Size (GB) [?]

Standard persistent disk 30

6. Seleccione la pestaña **Imágenes personalizadas** y la imagen del sistema creada anteriormente. Sus datos rellenan los menús **Mostrar imágenes del proyecto** y los menús desplegables **Tipo de disco de arranque y Tamaño (GB)**.
7. Haga clic en **Select**. Aparece la página **Crear una instancia** con la imagen del disco de arranque establecida en la imagen que acaba de seleccionar.
8. Seleccione **Permitir tráfico HTTPS**.

9. Amplíe la sección **Administración, seguridad, discos, redes y arrendamiento único** . Seleccione la pestaña **Discos** .

Additional disks ? (Optional)

New disk (gcp-elm-repo-disk, Blank, 300 GB)
🗑️ ⬆️

Name (Optional) ?
Name is permanent

Description (Optional)

Type ?

Standard persistent disk
▾

Snapshot schedule
Use snapshot schedules to automate disk backups. [Scheduled snapshots](#) ↗️

No schedule
▾

💡 Create snapshot schedules to automatically back up your data.
[Learn more about creating snapshot schedules](#) ↗️

Dismiss

Source type ?

Blank disk

Image

Snapshot

Mode

Read/write

Read only

Deletion rule
When deleting instance

Keep disk

Delete disk

Size (GB) ?

Estimated performance ?

Operation type	Read	Write
Sustained random IOPS limit	225.00	450.00
Sustained throughput limit (MB/s)	36.00	36.00

10. En la sección **Discos adicionales**, seleccione **+ Botón Agregar disco nuevo**.
11. Introduzca un nombre descriptivo.
12. En **Tipo de origen**, seleccione la pestaña **Disco en blanco** e introduzca el **Tamaño (en GB)** para el disco del repositorio.
13. Seleccione **Listo** para terminar de agregar un disco adicional.
14. En la sección Administración, seguridad, discos, redes, arrendamiento único, seleccione la pestaña **Redes**.

Management Security Disks **Networking** Sole Tenancy

Network tags ? (Optional)

Hostname ?
Set a custom hostname for this instance or leave it default. Choice is permanent

Network interfaces ?
Network interface is permanent

Network interface

Network ?
network-name-demo

Subnetwork ?
subnetwork-name-demo (———.0.0/20)

Primary internal IP ?
Ephemeral (Automatic)

⌵ Show alias IP ranges

External IP ?
None

IP forwarding ?
Off

Done Cancel

15. En la sección **Interfaz de red**, seleccione una **red**. Compruebe que aparezca un valor en el **campo Subrede** y seleccione un valor para él.

Importante:

Le recomendamos que no cree una dirección IP externa (pública).

16. (Recomendado) En el menú desplegable **IP externa**, selecciona **Ninguno**.
17. Seleccione **Listo** para finalizar la edición de la interfaz de red.
18. Seleccione **Crear** para crear la instancia de VM. Se crea la máquina virtual y el dispositivo se enciende. Una vez creado el dispositivo, ya no es necesario descargar el disco del sistema.
19. Para limpiar después de la instalación, retire:
 - El archivo.zip que has descargado.
 - Carpeta que contiene los archivos sin comprimir.
 - El archivo **unidesk_gcp-system.tar.gz** de la carpeta donde lo subió.

Si quiere que el dispositivo utilice una dirección IP estática

Puede cambiar la dirección IP del dispositivo y sus servidores DNS. Cuando el dispositivo se implementa por primera vez, la configuración de DNS se obtiene a través de DHCP. Si DHCP no está disponible y utiliza direcciones IP estáticas, una vez que seleccione **Estática**, se le pedirá que introduzca las direcciones IP de los servidores DNS.

1. Inicie sesión en la Utilidad de configuración del dispositivo mediante los pasos y la contraseña predeterminada descritos en [Configuración del dispositivo](#).
2. En la solicitud de acción, escriba **C** (para Configurar red) y presione Retorno.
3. En la siguiente solicitud, escriba **D** para Dinámica (DHCP) o **S** para estática.
Si elige Estático, se le pedirá la dirección IP y la máscara de subred, junto con las direcciones predeterminadas para las direcciones de puerta de enlace y DNS.
4. Cuando se le solicite, escribe **Y** para guardar la configuración.
5. En la solicitud de acción, escriba **Q** para salir.
6. Reinicie el dispositivo.

Siguientes pasos

Una vez instalado el dispositivo y la dirección IP está configurada correctamente, debe:

- [Instalar el agente de App Layering](#)
- [Configurar el servicio App Layering](#)
- [Acceso a la consola de administración de App Layering](#)

MS Azure o Azure Government

June 27, 2024

Para instalar el servicio App Layering, implemente el dispositivo en una máquina virtual mediante el administrador de recursos de Azure (o Azure Government).

- **Requisitos.** - Asegúrese de que dispone de los recursos de Azure (o Azure Government) que debe instalar el dispositivo.
- **Instale el dispositivo de App Layering en Azure (o Azure Government).** - Para instalar el dispositivo, descargue el paquete de instalación e implemente el dispositivo.
- **Pasos siguientes :** Enlaces a los pasos para instalar el agente de App Layering y configurar el servicio App Layering.

Nota: Si aún no ha configurado una conexión a una red virtual de Azure, consulte [Introducción a Azure o AzureGovernment](#) para obtener más información.

Los pasos para instalar el dispositivo en Azure y Azure Government son los mismos, además del script de instalación que ejecuta (los scripts se enumeran en el paquete de instalación a continuación).

Requisitos

Antes de instalar App Layering en Azure o Azure Government, asegúrese de tener lo siguiente.

- **Una cuenta y una suscripción de Azure**

Para implementar y configurar el dispositivo de App Layering, necesita las credenciales de una cuenta que tenga acceso administrativo a su suscripción de Azure. Para obtener más información, consulte la [página Inicio de sesión de Microsoft Azure](#).

- **Una red virtual en Azure (o Azure Government)**

Su implementación en Azure (o Azure Government) puede funcionar en una red virtual punto a sitio o sitio a sitio. El dispositivo y su recurso compartido de archivos de red deben tener conectividad de red. Sin embargo, el dispositivo no requiere conectividad de red a las imágenes en capas que publique. Se recomienda una conexión de sitio a sitio entre la empresa y las redes de Azure (o Azure Government) para acceder a la consola de administración del dispositivo. Para obtener más información, consulte la [página Red virtual de Microsoft Azure](#).

Nota: Si aún no ha configurado una conexión a una red virtual de Azure, consulte [Introducción a Azure para obtener](#) más información.

- **Un recurso compartido de archivos de red (detalles de Azure o Azure Government)**

Un servidor compartido de archivos en Azure (o Azure Government) funciona mejor que un recurso compartido de archivos local. Aunque la función Compartir archivos de Azure (o Azure

Government) no es compatible, puede usar un recurso compartido de archivos de red existente o crear un recurso compartido de archivos en el entorno de Azure (o Azure Government).

Importante: Se recomienda utilizar Premium Storage.

- **Administrador de recursos de Azure (o Azure Government)**

App Layering funciona con el modelo de administración de recursos (ARM) de Azure. No es compatible con el modelo de implementación clásico de Azure. Todos los recursos, como la red virtual, los recursos compartidos de archivos y las máquinas del sistema operativo con las que funcionará App Layering, deben crearse con Azure Resource Manager. Para obtener más información, consulte la [página de descripción general de Azure Resource Manager](#).

- **Azure PowerShell v7**

Azure PowerShell v7 debe instalarse en el sistema Windows que se utilizará para instalar el dispositivo en Azure.

- **Identidad gestionada asignada**

Se debe [asignar](#) al dispositivo App Layering una identidad gestionada para permitir la implementación en Azure.

Instalar el dispositivo de App Layering

Para implementar el dispositivo de App Layering en Azure o Azure Government:

1. Compruebe el contenido del paquete de instalación.
2. Obtenga información sobre lo que se incluye en el script de instalación.
3. Implemente el dispositivo.

Paquete de instalación

El paquete de instalación se denomina `citrix_app_layering_azure_yy.m.b`, donde:

`yy` es el año,
`m` (o `mm`) es el mes,
`b` es la compilación

Archivo	Descripción
<code>Azure_yy.m.b.zip</code>	Archivo VHD para la máquina virtual del dispositivo
<code>AzureELMDeploymentV7.ps1</code>	Script de instalación de Azure Government
<code>citrix_app_layering_agent_installer.exe</code>	Instalador del agente App Layering

Archivo	Descripción
citrix_app_layering_os_machine_tools.exe	Máquinas herramientas OS
DeployAzureRmVm.template.json	Plantilla de App Layering

Script de instalación

El script de instalación incluida en el paquete de instalación hace lo siguiente.

- Copia el VHD incluido en la ubicación de Azure que especifique.
- Crea una máquina virtual en Azure mediante el VHD,
- Adjunta el disco del repositorio.
- Bota el dispositivo Azure.

Cuando ejecuta el script:

- **IMPORTANTE:** Asegúrese de anotar la ubicación del grupo de recursos que seleccione, ya que necesitará esta información más adelante. Para obtener más información sobre los grupos de recursos, consulte [Uso de Azure Portal para administrar los recursos de Azure](#).
- Al seleccionar un tamaño de máquina virtual, se recomienda encarecidamente que seleccione una máquina con 4 CPU y al menos 14 GB de memoria (script predeterminada).
- El nombre que especifique para la nueva máquina virtual debe cumplir con las convenciones de nomenclatura de Azure.
- Seleccione una red virtual en la que se pueda acceder al puerto HTTP: 80 (se puede inhabilitar la IP pública).

Implementar el dispositivo en Azure o Azure Government

La descarga ZIP de App Layering requiere 31 GB de espacio cuando se descomprime.

1. Extraiga el paquete de descarga, citrix_app_layering_azure_yy.mm.zip. Los archivos incluidos se enumeran más arriba.
2. Extraiga el archivo ZIP en una carpeta de la unidad local.
3. Abra una ventana de Azure PowerShell.
4. Ejecute el script de instalación (incluido en el paquete de instalación) y responda a las indicaciones. Ejecutar el script:
 - Copia el VHD en la ubicación de Azure de su elección y conecta el disco del repositorio.
 - Reinicia el dispositivo.
 - Si el script falla, compruebe los valores para asegurarse de que los valores son correctos para su entorno.

La primera vez que inicie sesión en el dispositivo, deberá cambiar las contraseñas del administrador de App Layering. Para obtener más información, consulte [Cambiar contraseñas administrativas](#).

Asegúrese de instalar el agente App Layering, si su entorno lo requiere. Consulte la sección siguiente para obtener más información.

Siguientes pasos

Una vez instalado el dispositivo y la dirección IP esté configurada como quiere, puede instalar el agente App Layering y configurar el servicio App Layering:

- [Instalar el agente de App Layering](#)
- [Configurar el servicio App Layering](#)

MS Hyper-V

November 5, 2020

Para instalar el servicio App Layering, implemente el dispositivo en una máquina virtual en Hyper-V. Si el dispositivo requiere una dirección IP estática, debe configurarla mediante la utilidad de configuración del dispositivo, como se describe a continuación. En la última sección se describen los pasos siguientes.

Requisitos

Asegúrese de que la máquina virtual Hyper-V desde la que está instalando el dispositivo cumple los siguientes requisitos previos:

- Windows Server 2016, Windows Server 2012 R2
- Red virtual en Hyper-V

Descargue el paquete de instalación

Descargue el paquete de instalación, `citrix_app_layering_hyperv_4.x.x`, del sitio de descargas de [Citrix](#). El archivo zip incluye:

Archivo	Descripción
hyperv_arch.zip	VDHX para la VM del dispositivo
citrix_app_layering_agent_installer.exe	del agente de App Layering
citrix_installer.exe	de la máquina del SO

Configuración de la máquina virtual para el dispositivo

La máquina virtual que utilice para el dispositivo debe configurarse de la siguiente manera:

Nombre	Dispositivo	Generación	Memoria	Cantidad de CPU	Disco
la máquina virtual (Enterprise Layer Manager)	de la máquina virtual	de generación de la máquina virtual	8192 MB	4 CPU	1 system.vhdx

Implementar el dispositivo en Hyper-V

Para implementar el dispositivo:

1. Extraiga el paquete de descarga, citrix_app_layering_hyperv_4.x.x.zip. Se incluyen dos archivos de disco (vhdx).
2. Copie los discos en una ubicación de almacenamiento a la que pueda acceder el servidor de Hyper-V.
3. Abra el Administrador de Hyper-V, haga clic con el botón secundario en el servidor Hyper-V donde quiere implementar el dispositivo y seleccione **Nueva máquina virtual**.

4. En la primera ficha del asistente que se abre, haga clic en **Siguiente** para comenzar a configurar la máquina virtual.
5. En la ficha Especificar nombre y ubicación, defina el **nombre** y la **ubicación** de la nueva máquina virtual. Idealmente, use la ubicación donde extrajo los discos en el paso 2.
6. En la ficha Especificar generación, asegúrese de que las máquinas virtuales de generación 1 estén seleccionadas. Solo se admite la generación 1.
7. En la ficha Asignar memoria, configure la máquina virtual para que use 8 GB de RAM. Asegúrese de que la casilla de verificación **Usar memoria dinámica para esta máquina virtual** no está marcada.
8. En la ficha Configurar red, especifique la NIC que el adaptador de red utilizará para conectarse a la red.
9. En la ficha Conectar disco duro virtual, conecte el disco del sistema (**unidesk_hyperv-system.vhdx**), uno de los discos que extrajo en el paso 2.
10. En la ficha Resumen, compruebe las opciones y haga clic en **Finalizar**.
11. De vuelta en el Administrador de Hyper-V, seleccione la máquina virtual y haga clic en **Configuración en el panel** de la máquina virtual.
12. Seleccione **Hardware > Procesador** y establezca el Número de procesadores virtuales en 4.
13. Seleccione Controlador **IDE 0 > Disco duro**, haga clic en **Agregar**.
14. Seleccione el **botón de opción Disco virtual**, haga clic en **Examinar** seleccione el disco de repositorio (**unidesk_hyperv-repository.vhdx**) extraído en el paso 2.
15. Encienda la máquina virtual.
16. Escriba la dirección IP y el inicio de sesión de un administrador con permiso para acceder a la consola de administración de App Layering.

La primera vez que inicie sesión en el dispositivo, debe cambiar las contraseñas del administrador de App Layering. Para obtener más información, consulte [Cambiar contraseñas administrativas](#).

Configurar una dirección IP estática para el dispositivo, si es necesario

Puede cambiar la dirección IP del dispositivo y sus servidores DNS. Cuando el dispositivo se implementa por primera vez, la configuración de DNS se obtiene a través de DHCP. Si DHCP no está disponible y utiliza direcciones IP estáticas, una vez que seleccione **Estática**, se le pedirá que introduzca las direcciones IP de los servidores DNS.

1. Inicie sesión en la Utilidad de configuración del equipo, siguiendo los pasos y la contraseña predeterminada descritos en [Configuración del dispositivo](#).

2. En la solicitud de acción, escriba **C** (para Configurar red) y presione Retorno.
3. En el siguiente mensaje, escriba **D** para Dynamic (DHCP) o **S** para Static. Si elige Estático, se le pedirá la dirección IP y la máscara de subred, junto con las direcciones predeterminadas para las direcciones de puerta de enlace y DNS.
4. Cuando se le solicite, escriba **Y** para guardar la configuración.
5. En la solicitud de acción, escriba **Q** para salir.
6. Reinicie el dispositivo.

Siguientes pasos

Una vez instalado el dispositivo y la dirección IP está configurada correctamente, debe:

- [Instalar el agente de App Layering](#)
- [Configurar el servicio App Layering](#)

Nutanix AHV

April 8, 2021

Para instalar el servicio App Layering, implemente el dispositivo en una máquina virtual del hipervisor.

- **Requisitos.** Asegúrate de tener las cuentas, la configuración y los recursos necesarios de Nutanix.
- **Instale el dispositivo de App Layering en Nutanix.** - Para instalar el dispositivo, descargue el paquete de instalación e implemente el dispositivo en Nutanix.
- **Si el dispositivo necesita una dirección IP estática.** : puede establecer una dirección IP estática accediendo a la utilidad de configuración del dispositivo.
- **Próximos pasos.** - Enlaces a pasos para instalar el agente de App Layering y configurar el servicio App Layering.

Requisitos

Si está instalando el dispositivo y construyendo sus capas en máquinas virtuales de Nutanix, o está publicando imágenes en capas que se usarán en un entorno de Nutanix, necesitará los siguientes parámetros y recursos.

- **Cuenta y privilegios de Nutanix**
 - Una cuenta Nutanix AHV existente o nueva para usar en App Layering.

- La cuenta debe tener privilegios de Nutanix AHV para:
 - * Cree y elimine discos virtuales.
 - * Copiar y eliminar capas en discos virtuales mediante las API de archivos Nutanix.
- **Software y configuración de Nutanix:** Acceda a las herramientas de Nutanix para realizar instalaciones en la capa.
- **Información de recursos Nutanix** - La información enumerada en el [Configuración del conector de Nutanix AHV](#).

Instalar el dispositivo de App Layering en Nutanix AHV

Para implementar el dispositivo de App Layering en Nutanix:

- Verifique el contenido del paquete de instalación.
- Implemente el dispositivo.

Paquete de instalación

El paquete de instalación, citrix_app_layering_nutanix_4.x.x, incluye:

Archivo	Descripción
Nutanix_x.x.x.zip	Archivos IMG para la máquina virtual del dispositivo
citrix_app_layering_agent_installer.exe	Instalador del Agente de App Layering
citrix_app_layering_os_machine_tools.exe	Máquinas herramientas de SO

Implementar el dispositivo en Nutanix

1. Extraiga el paquete de descarga, citrix_app_layering_nutanix_4.x.x.zip. Los archivos incluidos se enumeran más arriba.
2. A continuación, descomprima el archivo zip nutanix_4.x.x, que contiene dos archivos IMG.
3. En la consola de Nutanix Prism, seleccione el menú **Herramientas** en la esquina superior derecha de la interfaz de usuario y elija **Configuración de imagen**.
4. Haga clic en el botón **Cargar imagen** y asigne un nombre al disco.
5. Seleccione el **Tipo de imagen de disco**.

6. Seleccione la opción **Cargar un archivo**, busque su recurso compartido de archivos y elija el disco de arranque de App Layering (IMG del “sistema”). Espere a que se complete la carga.
7. Repita los pasos 3 a 6 para el disco de almacenamiento local (IMG del “repositorio”).
8. Seleccione **Tareas** y asegúrese de que, para cada uno de los discos, se hayan completado las tareas *Crear imagen* y *Actualizar imagen*. Una vez hecho esto, puede crear la máquina virtual.
9. Seleccione la ficha **VM**(Máquina virtual) en el menú desplegable superior izquierdo y haga clic en el botón **Crear máquina virtual**.
10. Complete el **nombre** y la **descripción** de la nueva máquina virtual.
11. Establezca VCPU (S) en **1**.
12. Establezca el **número de núcleos por vCPU** en **4**.
13. Establezca la memoria en **8 GB**.
14. Para agregar los discos a la máquina virtual, haga clic en **Agregar nuevo disco** y elija el tipo **Disco**.
15. En el menú desplegable Operación, elija **Clonar desde Servicio de imágenes**.
16. En el menú desplegable **Tipo de bus**, seleccione **IDE**.
17. En el cuadro de imagen, seleccione el disco de arranque que cargó y haga clic en **Agregar**.
18. Repita los pasos 14 a 17 para cada uno de los siguientes discos:
 - Disco de arranque:** citrix_applayering_nutanix-system.img
 - Disco del repositorio:** citrix_applayering_nutanix-repository.imgAñada NIC haciendo clic en **Agregar nueva NIC**.
19. Haga clic en **Guardar** para crear la máquina virtual.
20. Encienda la máquina virtual.

Agregue el dispositivo Citrix App Layering a la lista de permitidos de Nutanix

Asegúrese de agregar el dispositivo a la lista de permisos de Nutanix para que el dispositivo pueda conectarse a Nutanix.

Si el dispositivo necesita una dirección IP estática

Puede cambiar la dirección IP del dispositivo y sus servidores DNS. Cuando el dispositivo se implementa por primera vez, la configuración de DNS se obtiene a través de DHCP. Si DHCP no está disponible y utiliza direcciones IP estáticas, una vez que seleccione **Estática**, se le pedirá que introduzca las **direcciones IP** de los servidores DNS.

1. Inicie sesión en la Utilidad de configuración del dispositivo mediante los pasos y la contraseña predeterminada descritos en [Configuración del dispositivo](#).
2. En la solicitud de acción, escriba C (para Configurar red) y presione Retorno.
3. En el siguiente mensaje, escriba **D** para Dinámico (DHCP) o S para Estático.
Si elige Estático, se le pedirá la dirección IP y la máscara de subred, junto con las direcciones predeterminadas para las direcciones de puerta de enlace y DNS.
4. Cuando se le solicite, escriba Y para guardar la configuración.
5. En la solicitud de acción, escriba Q para salir.
6. Reinicie el dispositivo.

Siguientes pasos

Una vez instalado el dispositivo y la dirección IP está configurada como desee, puede instalar el agente de App Layering, si es necesario, y configurar el servicio de App Layering. Consulte [Cuando se requiere el agente](#).

- [Instalar el agente de App Layering](#)
- [Configurar el servicio App Layering](#)

VMware vSphere

June 30, 2021

Para instalar el servicio App Layering, implemente el dispositivo en una máquina virtual del hipervisor.

Requisitos

El dispositivo de App Layering requiere la siguiente configuración de máquina virtual, los requisitos de vSphere y los permisos de vCenter.

Configuración de la máquina virtual

Al crear la máquina virtual del dispositivo, se requiere:

- 4 CPUs
- 8 GB de RAM

Requisitos de VMware vSphere

Para instalar el dispositivo de App Layering en un entorno VMware vSphere, necesita lo siguiente:

- [Una versión compatible de VMware vSphere.](#)
- Una red virtual en vSphere.
- Cuenta y privilegios de vCenter.

Necesita una cuenta de vCenter con permisos en un centro de datos para:

- Creación y eliminación de máquinas virtuales.
- Creación, copia y eliminación de discos de máquina virtual.

Además, la cuenta necesita este permiso en el nivel de vCenter:

- Eliminación de máquinas virtuales del inventario.

Para obtener más información, consulte la lista de [Permisos de vCenter](#) en la siguiente sección.

- El rol de App Layering que se aplicaría al centro de datos.

Para configurar un nuevo rol:

1. En vSphere Client, vaya a **Inicio > Administración > Funciones.**
 2. Haz clic en **Agregar rol.**
 3. Escriba un nombre. Por ejemplo: *CALAdmin*.
 4. Establezca los privilegios de la cuenta.
- Privilegios definidos para el rol de vCenter que está mediante para el servicio App Layering. Aplicar el nuevo rol al centro de datos que planea utilizar para App Layering. Para obtener más información, consulte la lista de [Permisos de vCenter](#) en la siguiente sección.
 1. Abra la ventana **Asignar permisos.**
 2. En el cliente vSphere, vaya a **Inicio > Inventario > Hosts y clústeres.**
 3. Seleccione su **centro de datos** y, a continuación, haga clic con el botón derecho y seleccione **Agregar permiso.**
 4. En la ventana **Asignar permisos**, en **Rol asignado**, expanda **Todos los privilegios.**
 5. Seleccione el requerido [Permisos de vCenter](#).
 6. Active la casilla **Propagar a objetos secundarios** y haga clic en **Aceptar.**
 - El rol de App Layering debe asignarse a la cuenta de administrador, de la siguiente manera:
 1. Agregue la cuenta de administrador y, a continuación, asígnele el rol de App Layering.
 2. Permitir que los permisos se propaguen a todo el centro de datos.

Nota: Si desea restringir a este usuario el acceso a carpetas específicas del centro de datos, conceda al usuario permisos más restrictivos para esas carpetas.

- Dado que el permiso **Máquina virtual > Inventario > Quitar** debe asignarse en el nivel de vCenter, debe crear un segundo rol.
 1. En vSphere Client, vaya a **Inicio > Administración > Funciones**.
 2. Haga clic en **Agregar rol** e introduzca un nombre; por ejemplo: CALAdmin-vmremove.
 3. Añade **máquina virtual > Inventario > Eliminary** deja todo lo demás configurado en *solo lectura*.
 4. En vSphere Client, vaya a **Inicio > Inventario > Hosts y clústeres**.
 5. Seleccione la pestaña **Permisos de vCenter**, haga clic con el botón derecho y seleccione **Agregar permiso** (o modifique los permisos de una cuenta existente).

Nota:

Asegúrese de usar la cuenta que tiene configurados los permisos del centro de datos.

6. Seleccione el nuevo rol CalAdmin-VMRemove que ha definido. Asegúrese de que la casilla de verificación Propagar a objetos secundarios está activada y, a continuación, haga clic en Aceptar.

Nota:

Si su directiva de seguridad lo permite, puede establecer todos los permisos en el nivel de vCenter en su lugar.

Permisos de vCenter

Expanda **Todos los privilegios**, a continuación, cada una de las siguientes categorías de permisos y seleccione los permisos necesarios. Los nombres de permisos pueden variar según la versión de VMware vSphere.

Nota:

A partir de la versión 19.11, ya no se requiere el permiso Host.Configuration.Administración del sistema.

Almacén de datos

- Asignar espacio
- Examinar almacén de datos
- Operaciones de archivos de bajo nivel

Carpeta

- Crear carpeta

Global

- Cancelar tarea

Red

- Asignar red

Recurso

- Asignar máquina virtual a la agrupación de recursos

vApp

- Export
- Import

Máquina virtual > Configuración

- Agregar disco existente
- Agregar nuevo disco
- Agregar o quitar dispositivo
- Avanzado
- Cambiar recuento de CPU
- Cambiar recurso
- Memoria
- Modificar parámetros de dispositivo
- Quitar disco
- Cambio de nombre
- Establecer anotación
- Parámetros
- Actualizar la compatibilidad de máquinas virtuales

Máquina virtual > Interacción

- Configurar medios de CD
- Interacción de consola
- Conectar dispositivos
- Apagado
- Encendido
- Restablecer
- Instalación de VMware Tools

Máquina virtual > Inventario

- Crear a partir de existentes

- Crear
- Remove

Máquina virtual > Aprovisionamiento

- Plantilla de clonación (opcional, pero necesaria para utilizar una plantilla de vSphere como máquina virtual de origen)
- Clonar máquina virtual

Máquina virtual > Administración de instantáneas

- Crear instantánea
- Revertir a instantánea
- Eliminar instantánea

Instalar el dispositivo de App Layering en VMware vSphere

Para implementar el dispositivo de App Layering en vSphere:

- Asegúrese de que tiene los requisitos de vSphere.
- Familiarícese con el contenido del paquete de instalación.
- Implemente el dispositivo.

Paquete de instalación

El paquete de instalación, `citrix_app_layering_vmware_21.4.x.x`, incluye:

Archivo	Descripción
<code>vmware_x.x.ova</code>	Archivo OVA para la máquina virtual del dispositivo
<code>citrix_app_layering_agent_installer.exe</code> que es	Instalador del Agente App Layering
<code>citrix_app_layering_os_machine_tools.exe</code> que es	Máquinas herramientas de SO

Implementar el dispositivo

1. Extraiga el paquete de descarga, `citrix_app_layering_vmware_21.4.x.x.zip`. Los archivos incluidos se enumeran al principio de este tema.
2. Extraiga `vmware_4.x.xx.ova` a una carpeta de la unidad local.
3. En vSphere Web Client que está utilizando, vaya a la página **VM y plantillas**.

4. Haga clic con el botón derecho en la carpeta de vSphere en la que desea desplegar la plantilla y seleccione **Implementar plantilla OVF**. Aparece el asistente Deploy OVF Template.
5. En el asistente Implementar plantilla de OVF, haga lo siguiente:
 - a) En la página **Seleccionar origen**, seleccione la opción **Archivo local** y vaya al archivo **vmware_x.x.x.ova** para seleccionarlo.
 - b) En la página **Seleccionar nombre y carpeta**, designe un nombre y una ubicación para la plantilla OVF implementada.
 - c) En la página **Seleccionar un recurso**, seleccione una ubicación para ejecutar la plantilla OVF implementada.
 - d) En la página **Seleccionar almacenamiento**, seleccione la configuración **Aprovisionamiento grueso Lazy Zeroed** de la opción **Seleccionar formato de disco virtual**, seleccione una directiva de almacenamiento y especifique una ubicación de almacenamiento.
 - e) En la página **Configurar redes**, seleccione la red virtual de vSphere en la columna **Destino** y seleccione la configuración **IPv4** de la opción de **protocolo IP**.
 - f) En la página **Listo para completar**, revise la configuración de la plantilla y, a continuación, haga clic en **Finalizar** cuando esté satisfecho con la configuración.

Si el dispositivo necesita una dirección IP estática

Puede cambiar la dirección IP del dispositivo y sus servidores DNS. Cuando el dispositivo se implementa por primera vez, la configuración de **DNS** se recupera mediante el Protocolo de configuración dinámica de host (DHCP)}. Si DHCP no está disponible, puede usar direcciones IP estáticas. Seleccione **Estática** e introduzca las **direcciones IP** de los servidores DNS.

1. Inicie sesión en la Utilidad de configuración del dispositivo mediante los pasos y la contraseña predeterminada descritos en [Configuración del dispositivo](#).
2. En la solicitud de acción, escriba C (para Configurar red) y presione Retorno.
3. En la siguiente solicitud, escriba **D** para DHCP o **S** para estática. Si elige **Estática**, se le pedirá lo siguiente:
 - **Dirección IP**
 - **Máscara de subred**
 - **Dirección de puerta de enlace predeterminada**
 - **Dirección DNS predeterminada**
4. En la siguiente solicitud, escriba **Y** para guardar la configuración.
5. En la solicitud de acción, escriba **Q** para salir.
6. Reinicie el dispositivo.

Siguientes pasos

Una vez instalado el dispositivo y configurada la dirección IP, proceda a:

- [Instalar el agente de App Layering](#)
- [Configurar el servicio App Layering](#)

Instalar el agente de App Layering

October 21, 2021

El agente App Layering permite que el dispositivo o un equipo de empaquetado ejecuten comandos de PowerShell localmente. Si proporciona las credenciales adecuadas, el agente puede ejecutar comandos de PowerShell como un usuario específico.

Cuando se requiere el agente

El agente App Layering es necesario si tiene previsto:

- Inicie scripts mediante las configuraciones de conectores.
- Ejecute el dispositivo de App Layering en Microsoft Hyper-V.
- Publique imágenes en capas en Citrix Provisioning.

Instalar el agente en las siguientes ubicaciones:

- En todos los servidores Hyper-V que planea utilizar para la creación de capas o la publicación de imágenes.
- En todos los servidores de Citrix Provisioning en los que tenga previsto publicar imágenes en capas.
- En ubicaciones donde las configuraciones de conectores ejecutan scripts de PowerShell.

Registrar el agente con el dispositivo

El instalador del agente de App Layering le pide que registre el agente con un dispositivo de App Layering. Si no registra el agente durante la instalación, puede registrarlo manualmente más tarde. Sin embargo, los scripts de PowerShell no se ejecutan hasta que el agente se registra con el dispositivo.

Requisitos previos

Antes de instalar el agente App Layering, asegúrese de que el sistema en el que está instalando el agente cumple los siguientes requisitos:

- Una cuenta con privilegios de administrador
- .NET 4.5
- PowerShell 3.0 o una versión posterior
- Complemento PowerShell. Antes de utilizar el agente App Layering en un servidor de Citrix Provisioning Services, debe asegurarse de que el complemento PowerShell esté instalado. Consulte los pasos para [registrar manualmente el agente](#) en el dispositivo.

Si instaló anteriormente el agente App Layering, puede descargar versiones actualizadas desde la página de descargas de Citrix. El paquete de instalación del agente se incluye en la descarga ZIP de App Layering.

Para descargar el agente App Layering

1. Vaya a la [página principal de Citrix](#) y, a continuación, haga clic en **Iniciar sesión**.
2. Haga clic en **Descargas** y seleccione **Citrix App Layering** de la lista.
3. En la página Citrix App Layering, en **Citrix App Layering > Software de producto**, haga clic en Citrix App Layering.
4. En la parte inferior de la página, haga clic en **Herramientas**.
5. Haga clic en el agente de Citrix App Layering **Descargar archivo**.
El archivo citrix_app_layering_agent_installer.exe se descarga a su equipo.

Instalar el agente de App Layering

El instalador del agente de App Layering le pide que registre el agente con un dispositivo de App Layering. Si no registra el agente durante la instalación, puede registrarlo manualmente más tarde. Sin embargo, tenga en cuenta que el agente debe estar registrado en el dispositivo antes de que se puedan ejecutar los scripts de PowerShell.

1. Con una cuenta con privilegios de administrador, inicie sesión en el sistema donde está instalando el agente.
2. Copie el archivo Citrix_app_layering_agent_installer.exe en una ubicación conveniente del servidor.
3. Ejecute Citrix_app_layering_agent_installer.exe como administrador y, cuando se le solicite, escriba la ruta al directorio en el que quiere instalar el agente App Layering. La ubicación predeterminada es C:\Program Files (x86)\Citrix\Agent.

El instalador del agente comprueba que todos los requisitos previos están presentes. Si falta algún requisito previo, el instalador lo informa y sale sin necesidad de instalarlo.

4. El instalador le solicita un número de puerto del agente. Puede aceptar el número de puerto predeterminado (8016) o especificar uno diferente si el puerto predeterminado ya está en uso.
5. El instalador le solicita las credenciales (dirección, nombre de usuario y contraseña) del dispositivo de App Layering. Registre el agente App Layering con el dispositivo introduciendo la dirección IP y las credenciales de inicio de sesión de un usuario de la consola de administración en el dispositivo con privilegios de administrador (por ejemplo, las credenciales que utiliza para iniciar sesión en la consola de administración).

Nota:

Si el dispositivo de App Layering no está disponible o decide no registrarse con él ahora, puede registrarse manualmente más adelante mediante el procedimiento descrito en Registrar con el dispositivo de App Layering manualmente.

6. Haga clic en **Finalizar** para salir del asistente.

registrar manualmente el agente App Layering con el dispositivo

Registre el agente App Layering con el dispositivo.

Si el agente de App Layering no está registrado en un dispositivo de App Layering durante la instalación, puede registrarlo más adelante mediante el procedimiento siguiente.

1. Como administrador, inicie sesión en el servidor donde instaló el agente App Layering.
2. Abra una ventana de comandos (cmd.exe) como administrador y navegue hasta el directorio donde está instalado el Agente de App Layering. La ubicación predeterminada es C:\Program Files (x86)\Citrix\Agent.
3. Ejecute el siguiente comando de PowerShell:

```
Enable-PSRemoting
```

4. Compruebe que el puerto 8016 está abierto ejecutando este comando:

```
netstat -a
```

5. Abra una ventana de comandos (cmd.exe) como administrador y navegue hasta el directorio donde está instalado el Agente de App Layering. La ubicación predeterminada es:

```
C:\Program Files (x86)\Citrix\Agent
```

6. Ejecute el siguiente comando, mediante la dirección IP del dispositivo donde se indique:

```
1 Citrix.AppLayering.Agent.Service.exe register /i /e:  
   IP_address_of_appliance /u:Administrator  
2 <!--NeedCopy-->
```

7. Cuando se le solicite, escriba la contraseña de un usuario que tenga privilegios de administrador en la consola de administración del dispositivo.
8. Cuando finaliza el proceso de registro, aparece un mensaje informándole del resultado correcto. El registro del agente de App Layering aparece en el registro de auditoría del servicio de administración.

Si el proceso no se realiza correctamente, examine el archivo de registro del agente en el directorio de instalación:

```
C:\Program Files (x86)\Citrix\agent\Logs\aplayering.agent.log
```

También puede ver la Ayuda para las opciones de línea de comandos del agente App Layering ejecutando el siguiente comando:

```
Citrix.AppLayering.Agent.Service.exe /?
```

9. Ejecute el comando PowerShell para cargar los archivos DLL correspondientes en Citrix Provisioning Server.

Para PVS 7.7 y versiones posteriores:

- a) Desplácese hasta:

```
C:\program files\citrix\provisioning services console
```

- b) Ejecute el comando:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.  
exe Citrix.PVS.snapin.dll
```

Para PVS 7.1—7.6:

- a) Desplácese hasta:

```
C:\program files\citrix\provisioning services console
```

- b) Ejecute el comando:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.  
exe McliPSSnapIn.dll
```

En caso de que algunos complementos de Citrix Provisioning y Broker no estén registrados, por ejemplo, después de una actualización importante de Windows, averigüe cuáles.

10. Ejecute el siguiente comando para enumerar los complementos registrados:

```
get-pssnapin -registered
```

11. Consulte este [artículo](#) para obtener instrucciones sobre cómo volver a registrar todos los complementos.

Configurar

May 9, 2024

Una vez que haya instalado el software App Layering e implementado el dispositivo, podrá [acceder a la consola de administración](#) que se ejecuta en el dispositivo.

Para proteger el dispositivo, debe [establecer sus propias contraseñas de administrador](#) la primera vez que inicie sesión en la consola. A continuación, puede proceder a:

- [Configurar un recurso compartido de archivos](#)
- [Conectarse a un servicio de directorios](#)
- [Asignar roles a usuarios](#)

También tiene la oportunidad de [habilitar las funciones de Labs](#) que se están probando actualmente.

Consola de administración de acceso

July 6, 2022

Puede acceder al dispositivo de App Layering introduciendo la dirección IP del dispositivo en un explorador web.

La primera vez que inicie sesión en la consola de administración, usted:

- Introduzca el nombre de usuario (**administrador**) y la contraseña (**Unidesk1**) predeterminados.
- Acepte el acuerdo de licencia de Citrix.
- Cambie todas las contraseñas administrativas del dispositivo.

Acceder a la consola de administración

Para iniciar sesión directamente en la consola de administración alojada en el dispositivo App Layering:

1. En el hipervisor, busque la máquina virtual que creó para el dispositivo y determine su dirección IP.
2. Mediante la dirección IP del dispositivo, introduzca la siguiente dirección URL en un explorador web compatible:

`http://<ip_address_of_new_vm>`

3. Inicie sesión en la consola de administración. Introduzca el nombre de usuario y la contraseña predeterminados enumerados en la introducción.

La primera vez que alguien inicia sesión en la consola de administración de un dispositivo nuevo, el sistema fuerza un cambio de contraseña para cada una de las cuentas administrativas del dispositivo.

Importante:

Asegúrese de registrar las nuevas contraseñas en un lugar seguro, de acuerdo con las directrices de seguridad de su empresa.

Cambiar contraseñas de administrador

July 6, 2022

El dispositivo tiene tres cuentas que puede utilizar para administrar sus funciones y configuraciones.

- **Cuenta de “administrador” de la consola** de administración: le permite acceder a la consola de administración alojada en el dispositivo. Allí puede crear y administrar capas, y publicar imágenes en capas. La contraseña predeterminada es **Unidesk1**.
- **Cuenta de “administrador” del dispositivo**: Le permite acceder a la utilidad de configuración del dispositivo, donde puede cambiar la configuración de red, la fecha, la hora, el servidor NTP y la zona horaria. La contraseña predeterminada es **Unidesk1**.
- Cuenta de **usuario “root” del dispositivo**: la cuenta de superusuario de Linux predeterminada del dispositivo. La contraseña de esta cuenta es necesaria si alguna vez restablece sus otras cuentas administrativas. El usuario raíz tiene acceso a todos los comandos y archivos del sistema operativo Linux del dispositivo. La contraseña predeterminada es **v9Yx*6uj**.

La cuenta de administrador de la consola de administración es la más utilizada. Puede configurar y utilizar fácilmente el servicio App Layering sin tener que acceder a las otras dos cuentas.

Importante:

Guarde la contraseña del usuario root en un lugar seguro. Si lo necesita para restablecer las contraseñas de las otras dos cuentas de administrador.

Para proteger el dispositivo, debe cambiar las contraseñas de estas cuentas la primera vez que acceda a la consola de administración después de la instalación.

La primera vez que accede al dispositivo después de la instalación

Cuando se instala el dispositivo y se inicia sesión por primera vez, se muestra una ficha en la que *debe* cambiar las contraseñas de las cuentas de administrador que utiliza para administrar el dispositivo.

1. Para cada cuenta, introduzca la nueva contraseña y vuelva a escribirla en el campo Confirmar contraseña.
2. En la ficha Confirmar y completar, haga clic en **Cambiar credenciales**.
3. Almacene estas contraseñas de forma segura en caso de que las necesite.

ADVERTENCIA:

Debem mantener la contraseña del usuario **raízen** en una ubicación segura. Sin él, no podrá restablecer sus otras cuentas de administrador.

Para cambiar la contraseña de una cuenta administrativa

1. Inicie sesión en la consola de administración.
2. Vaya a **Sistema > Administradores > Administrador predeterminado**.
3. Haga clic en el botón **Modificar**.
4. Introduzca y confirme la nueva contraseña y haga clic en **Confirmar y completar**.

Configurar el recurso compartido de archivos

July 6, 2022

El dispositivo de App Layering debe estar conectado a un recurso compartido de archivos. Si aún no ha configurado un recurso compartido de archivos, siga estas instrucciones.

Puede agregar ubicaciones de almacenamiento para los datos y la configuración persistentes de los usuarios. También puede agregar espacio a los discos de almacenamiento que ya están en uso. Para

obtener más información sobre la administración del almacenamiento, consulte el artículo sobre la administración del [almacenamiento](#).

Si utiliza más de un dispositivo, cada dispositivo debe usar un recurso compartido de archivos diferente o una carpeta única en el mismo recurso compartido.

Requisitos

Al configurar el recurso compartido de archivos del dispositivo:

- El recurso compartido de archivos debe configurarse mediante la tecnología Bloque de mensajes de servidor (SMB).
- La cuenta de servicio que utiliza el dispositivo App Layering para conectarse al recurso compartido de archivos debe tener **permisos completos** para ese recurso compartido de archivos.
- Los usuarios requieren acceso de **solo lectura** al recurso compartido de archivos. Si planea [habilitar las capas de usuarios en las imágenes que publica](#), establezca también los permisos de uso compartido de archivos detallados en [Configurar la seguridad en las carpetas de capas de usuarios](#).
- Asegúrese de que tiene el requisito de espacio de almacenamiento mínimo de 40-100 GB para el recurso compartido de archivos.

Nota: El espacio de almacenamiento es ampliable. Puede agregar espacio a un disco o agregar otros discos al dispositivo.

Crear el recurso compartido de archivos de red

Configure un recurso compartido de archivos que utilice el protocolo SMB.

- Siga las instrucciones del proveedor para configurar un recurso compartido de archivos mediante el protocolo SMB.

Configurar el dispositivo de App Layering para acceder al recurso compartido de archivos

Una vez que haya creado un recurso compartido de archivos, configure el dispositivo App Layering para que lo adjunte. Puede configurar el dispositivo a través de la consola de administración de App Layering.

1. En Management Console, seleccione **Sistema > Recursos compartidos de archivos de red** y haga clic en **Modificar**.
2. Especifique una ruta del recurso compartido de archivos SMB, un nombre de usuario y una contraseña para el recurso compartido de archivos.

3. Haga clic en **Confirmar y completar** para ver si puede conectarse al recurso compartido de archivos. El recurso compartido de archivos se guarda si la conexión se realiza correctamente o muestra un error si se produce un error en la conexión.

Conectarse a un servicio de directorios

November 22, 2022

Puede configurar el dispositivo Citrix App Layering para que se conecte a Active Directory. Cuando se conecta al servicio de directorios, se crean uno o más cruces de directorio para acceder a dominios o unidades organizativas (OU) específicos.

El dispositivo *no* modifica el servicio de directorio al que se conecta. El software almacena en caché los atributos de cada entrada de servicio de directorios. Si la conexión al servicio de directorios se pierde temporalmente, el software puede utilizar la información almacenada en caché para tareas de administración.

Al crear una unión de directorios, utilice las siguientes siglas estándar del sector:

- OU: Unidad organizativa
- DC: Componente de dominio

Acerca de la conexión del dispositivo a un servicio de directorios

Qué sucede cuando se agregan los cruces de directorio

Cada cruce de directorios que cree especifica un nodo inicial en el árbol de directorios. Una nueva unión de directorio no puede incluir usuarios que ya son miembros de otra unión. No puede anidar cruces.

Si va a crear varios nombres distintivos

El sistema compara primero el componente de dominio; las partes del nombre distinguido que comienzan con “DC =”.

En Nombres Distinguidos, el orden importa. Por ejemplo, DC = A, DC = B es diferente de DC = B, DC = A.

El sistema agrega cruces de directorio En los siguientes casos:

- Los componentes del dominio difieren.

- Sus componentes de dominio coinciden y los componentes restantes no se superponen.

Los cruces de directorio se fusionan si los componentes de dominio coinciden y los demás componentes están relacionados.

Los atributos de usuario se importan desde el servicio de directorios

El software de App Layering importa y almacena en caché los atributos de usuario y grupo de su servicio de directorios cuando:

- Asignar privilegios de administrador a un usuario.
- Los valores de los atributos cambian en el servicio de directorios.

Los atributos que almacena en caché de software son de solo lectura. Todos los cambios en los atributos para los usuarios del servicio de directorios provienen del servidor de directorios.

Los atributos importados se sincronizan regularmente

El software sincroniza la información que almacena en caché para los usuarios del servicio de directorios con el servicio de directorios cada 12 horas. Si un usuario ya no es un objeto en el servicio de directorio, el usuario se considera abandonado. Puede ver esta información en la vista Información del usuario.

Para crear una unión de directorio

1. Haga clic en **Sistema > Servicios de directorio**.
2. Haga clic en **Agregar cruce de directorios**.
3. Especifique los detalles del servidor de directorios:
 - **Dirección del servidor:** El nombre del servidor que utiliza para el servicio de directorio (dirección IP o nombre DNS).
 - **Puerto:** Especifique el número de puerto para comunicarse con el servidor de directorios.
 - **Usar SSL:** Haga clic para habilitar la comunicación de capa de sockets seguros (SSL). Si se producen errores de certificado, el asistente muestra una lista de estos errores. Si está seguro de que es seguro ignorarlos, haga clic en **Ignorar errores de certificado**.
 - **Conectar:** Haga clic para comprobar si el dispositivo se puede conectar al servicio de directorio.
 - **Nombre distinguido (DN) de enlace:** Para determinar la sintaxis correcta para el nombre de usuario o el nombre de usuario de enlace, consulte la documentación de su directorio. En los ejemplos siguientes se muestran algunas de las formas en que se puede especificar un usuario para el servicio de directorios:

- domain\username
 - [username@domain.com](#).
 - **Contraseña** de enlace: escriba la contraseña.
 - **Conectar**: Haga clic para comprobar si el dispositivo se puede conectar al servicio de directorio.
 - **Nombre distintivo base**: Especifique dónde comienza el software a buscar usuarios y grupos en el servicio de directorio remoto.
 - **Nombre de cruce de directorios**: El nombre de la carpeta que se ve en la vista de árbol. Puede utilizar cualquier nombre, incluido el nombre de un dominio en el árbol de servicios de directorios.
4. Haga clic en **Confirmar y completar**.

Asignar roles

June 29, 2023

Los roles de App Layering definen qué módulos de App Layering (funciones) puede administrar un usuario. Los usuarios asignados a uno o más roles pueden iniciar sesión en la consola de administración. Estos usuarios aparecen en la ficha **Sistema > Control de acceso**.

Usuarios, derechos y roles de App Layering

El servicio App Layering admite dos tipos de usuarios:

- **Administrador de App Layering**. Esta cuenta es exclusiva de App Layering. Lo recibirá cuando instale por primera vez el dispositivo App Layering e inicie sesión en la consola de administración. Puede usarlo para empezar. Esta cuenta de administrador “integrada” tiene los derechos para realizar *todas las* operaciones de App Layering. Puede modificar las propiedades de este administrador, incluidos el nombre, la contraseña y la información de contacto. La primera vez que inicie sesión en el dispositivo, deberá cambiar la contraseña de este administrador y aceptar el CLUF.
- **Usuarios de Active Directory (AD)**. Además de la cuenta de administrador integrada, todos los usuarios de App Layering son usuarios de AD importados a través de uno o más cruces de directorios. Una vez que se hayan creado los cruces de directorios, puede conceder otros derechos a los usuarios. Para obtener más información, consulte [Conectarse a un servicio de directorio](#).

Derechos y funciones

Puede seleccionar todos los derechos y roles de cada usuario al marcar estas casillas de verificación. Si selecciona **Administrador** o **Lector**, todas las demás casillas aparecerán atenuadas.

- **Lector:** Puede iniciar sesión en la consola de administración de App Layering, pero no puede modificar nada.
- **Colaborador de capas de aplicaciones:** Puede agregar, modificar y eliminar capas y versiones de aplicaciones.
- **Colaborador de capas del sistema operativo:** Puede agregar, modificar y eliminar capas y versiones del sistema operativo.
- **Colaborador de capas de plataforma:** Puede agregar, modificar y eliminar capas y versiones de plataforma.
- **Colaborador de plantillas de imágenes:** Puede agregar, modificar y eliminar plantillas de imágenes.
- **Editor de imágenes:** Puede publicar imágenes.
- **Colaborador de asignaciones de capas elásticas:** Puede agregar, modificar y eliminar asignaciones de capas elásticas.
- **Administrador:** Puede hacerlo todo.
- **Importador de capas:** Puede importar capas de sistema operativo, capas de aplicaciones y capas de plataforma desde fuentes externas.
- **Exportador de capas:** Puede exportar capas de sistema operativo, capas de aplicaciones y capas de plataforma a una ubicación externa.
- **Colaborador de conectores de plataforma:** Puede agregar, modificar y eliminar configuraciones de conectores de plataforma.
- **Exportador de registros:** Puede exportar y descargar el paquete de registro de App Layering.

Credenciales de usuario para iniciar sesión en la consola de administración

Al asignar roles a los usuarios del Servicio de directorios, pueden usar sus credenciales de servicio de directorios para iniciar sesión en la consola de administración.

¿Quién puede asignar roles de App Layering?

Puede cambiar la función de un usuario si ha iniciado sesión en la consola de administración como un usuario asignado a la función Administrador.

Asignar roles de App Layering a usuarios

1. Inicie sesión en la consola de administración.

2. Seleccione **Sistema > Control de acceso**.
3. Seleccione un usuario y haga clic en **Modificar**. Se abre la hoja Modificar usuario.
4. Elija los roles del usuario seleccionado.
5. Haga clic en **Confirmar y completar** y, a continuación, en **Guardar**.

Actualizaciones

May 30, 2023

Para conocer las últimas correcciones y funciones, incluida la compatibilidad con otros paquetes de software que utilice, le recomendamos que se mantenga actualizado con las actualizaciones de App Layering. El proceso de actualización está parcialmente automatizado, en el sentido de que el dispositivo comprueba periódicamente el paquete más reciente. Descarga nuevos paquetes, verifica y extrae los archivos. Los usuarios recibirán un mensaje la próxima vez que inicien sesión y los administradores con los permisos adecuados pueden iniciar la actualización.

Además de actualizar el dispositivo App Layering, también se espera actualizar:

- Agente de App Layering, si está instalado en el hipervisor y los servidores de Provisioning.
- Imágenes publicadas en capas (requiere el Provisioning de los servidores con las imágenes).

En este artículo se explica cómo completar cada una de las actualizaciones asociadas.

Antes de actualizar la versión

Antes de actualizar:

- Compruebe que está configurado un recurso compartido de archivos de red.
- Realízate del dispositivo.
- Compruebe la ruta de actualización compatible (solo para versiones anteriores a 19.1)

Compruebe que se ha configurado un recurso compartido de archivos de red

Para confirmar el recurso compartido, inicie sesión en el dispositivo y vaya a **Sistema > Uso compartido de archivos de red**. Después de asegurarse de haber configurado el recurso compartido de archivos, puede actualizar el dispositivo.

Realízate del dispositivo

Tome una instantánea o un punto de control del dispositivo.

Compruebe la ruta de actualización admitida

Si está actualizando desde una versión anterior del producto, utilice la siguiente ruta de actualización para actualizar la versión instalada. Haga clic en el número de versión para ir a la página de descargas de esa versión.

Actualizar desde la versión	A la versión
4.1	4.15
4.7	4.15
4.15	19.1
19.1	19.7
19.7	20.1
20.1	20.8
20.8	20.11
20.11	21.4
21.4	21.7
21.7	23.4

Actualizar el dispositivo

Las actualizaciones App Layering están parcialmente automatizadas. El dispositivo comprueba periódicamente si hay actualizaciones y descarga la última, siempre y cuando se disponga de los permisos correctos y de otros requisitos.

La carpeta **Actualización** incluye la actualización del dispositivo, la actualización del agente y una carpeta de herramientas para usar en la capa del sistema operativo.

Qué sucede si se encuentra una actualización

Si se encuentra una actualización durante la comprobación automática, se descargará en el dispositivo la carpeta comprimida más reciente disponible. El dispositivo verifica la descarga y extrae los archivos en segundo plano.

Mientras tanto, cada usuario recibe uno de los siguientes mensajes la próxima vez que inicie sesión:

- **Iniciar actualización:** ejecute la actualización del software del dispositivo App Layering (solo administradores).
- **Cerrar:** omita el mensaje para que pueda iniciar manualmente la actualización más adelante mediante la **ficha Usuario > Actualizar dispositivo**.

Para obtener más información sobre lo que comprueba el dispositivo, consulte [Cómo funcionan las comprobaciones de actualización, en detalle](#).

Quién puede iniciar la actualización

Solo un administrador puede iniciar la actualización.

Si el firewall impide las descargas automáticas del paquete de actualización

Si los requisitos del firewall impiden la descarga automática, descargue el paquete de actualización desde el sitio de descargas de Citrix. Copie el paquete en el archivo de red en el que el dispositivo puede acceder a él.

1. Desplácese hasta el archivo.zip y extraiga los archivos.
2. Inicie sesión en la consola de administración, seleccione **Usuario** y, a continuación, haga clic en **Actualizar dispositivo**.
3. Compruebe la ruta de actualización y haga clic en **Actualizar**. El proceso de actualización se inicia y abre una página de estado en el explorador.
4. Cuando se completa la actualización, el estado cambia a Estado de la **actualización: Completado**. Actualice la página web para volver a la consola de administración.
5. Compruebe que la actualización se realizó correctamente haciendo clic en el enlace **Acerca** de en la consola de administración para confirmar el número de versión.

Si va a actualizar desde App Layering 18.12 o anterior (solo VMware vSphere)

A partir de la versión 18.12, los botones **TEST** y **SAVE** comprueban los privilegios de VMware vSphere. Un pase significa que el dispositivo tiene permisos para crear, modificar y eliminar máquinas virtuales.

Si se actualiza desde la versión 18.12 o anterior, se espera establecer algunos permisos más que ahora son necesarios. Cree otro rol y asigne los permisos en el nivel de vCenter.

Crear otro rol Dado que el permiso de **Máquina virtual > Inventario > Eliminar** debe asignarse a nivel de vCenter, debe crear otro rol.

1. En vSphere Client, vaya a **Inicio > Administración > Funciones**.
2. Haga clic en **Agregar función** e introduzca un nombre, por ejemplo: **CALAdmin-vmremove**.
3. Agregue solo **Máquina virtual > Inventario > Eliminar**. Todo lo demás puede seguir siendo de *solo lectura*.
4. En vSphere Client, vaya a **Inicio > Inventario > Hosts y clústeres**.
5. Seleccione la ficha **Permisos de vCenter**, haga clic con el botón derecho y seleccione **Agregar permiso** (o modifique los permisos de una cuenta existente).

Nota:

Asegúrese de que la cuenta es la que posee los permisos del centro de datos establecidos anteriormente.

6. Seleccione la nueva función **CALAdmin-vmremove** que definió. Asegúrese de que la casilla de verificación Propagar a objetos secundarios está activada y, a continuación, haga clic en Aceptar.

Nota:

Puede establecer todos los permisos en el nivel de vCenter, si la directiva de seguridad lo permite.

Habilitar permisos de vCenter Habilite los permisos que se enumeran en el [artículo Instalar dispositivo en vSphere](#).

Inhabilite los siguientes parámetros Para su referencia, asegúrese de inhabilitar estos parámetros:

- vApp
 - Configuración de la aplicación
- Máquina virtual
 - Configuración
 - * Configuración avanzada
 - * Seguimiento de cambios
 - * Gestionado por
 - * Restablecer información de invitado
 - * Colocación de intercambio

- Interactuar
 - * Pregunta de respuesta
 - * Interactuar Consola
 - * Suspende
- Inventory
 - * Registrarse
 - * Anular registro
- Provisioning
 - * Personalizar
 - * Implementar plantilla
 - * Marcar como plantilla
- State
 - * Quitar instantánea

Actualizar el agente de App Layering (si está instalado)

A continuación, actualice el agente de App Layering. Este componente permite que un dispositivo o una máquina de empaquetado ejecuten comandos de PowerShell localmente. Puede esperar encontrar el agente instalado en las siguientes ubicaciones, si existen en su entorno:

- Servidores Hyper-V que App Layering utiliza para la creación de capas o la publicación de imágenes.
- Servidores de Citrix Provisioning en los que se publican imágenes en capas.
- Servidores en los que una configuración de conector ejecuta scripts de PowerShell. Para ver cualquier configuración de conector existente, abra la consola de administración y seleccione **Sistema > Conectores**.

Para actualizar el agente de App Layering en esas ubicaciones:

1. Copie el archivo de actualización del agente en los servidores donde está instalado el agente.
2. Haga doble clic en el archivo de actualización del agente y siga las instrucciones para actualizar el agente.

Actualizar las imágenes en capas publicadas

Las actualizaciones de App Layering incluyen actualizaciones de controladores, nuevas funciones y las correcciones de errores documentadas en [Novedades](#). Una vez que actualice el dispositivo, actualice las imágenes publicadas.

Para actualizar sus imágenes publicadas, seleccione cada una de sus plantillas de imagen, verifique la configuración y la use para **publicar** nuevas versiones de las imágenes en capas. Utilice las nuevas imágenes para aprovisionar sus sistemas.

Para aplicar la actualización a las imágenes en capas publicadas:

1. Inicie sesión en la consola de administración de capas.
2. Seleccione la ficha Imágenes. Se muestran las plantillas de imagen.
3. Si quiere verificar o actualizar la configuración de una plantilla, seleccione la plantilla de imagen y haga clic en **Modificar plantilla**. Modifique la configuración y haga clic en **Guardar plantilla y publicar**.
4. Si la plantilla de imagen *no* necesita edición, simplemente seleccione la plantilla y haga clic en **Publicar imagen en capas**.
5. Una vez publicadas, utilice las nuevas imágenes en capas para aprovisionar sus sistemas.

Antecedentes: Cómo funcionan las comprobaciones de actualización, en detalle

Cuando el dispositivo de App Layering comprueba si hay una actualización:

- **Si no hay una actualización disponible:** no ocurre nada. Otra comprobación se realiza en el siguiente intervalo programado.
- **Si hay una actualización disponible, pero no hay ningún recurso compartido de archivos de red configurado:** el usuario recibe un mensaje que indica que hay una actualización disponible. Le pide que termine de configurar el recurso compartido de archivos de red.
- **Si hay una actualización disponible:** se inicia un trabajo para “Descargar medios de actualización”. Puede comprobar el progreso a través de las siguientes tareas:
 - Descarga de los medios de actualización al almacenamiento local.
 - Asegurarse de que la suma de comprobación del paquete de actualización descargado correctamente sea correcta.
 - Extraer el paquete de actualización descargado al recurso compartido de archivos de red configurado. La descarga se extrae en el recurso compartido de archivos del dispositivo:
Ubicación: `NetworkFileShare*AppLayeringVersion*`
Ejemplo: `\MyServer\AppLayeringFileShare\4.0.8`
 - * Si la extracción se realiza correctamente, la próxima vez que un usuario inicie sesión se le notificará que hay una actualización disponible.
 - * Si en algún momento durante este proceso un error requiere la intervención del administrador, el trabajo falla con un error. Por ejemplo:
 - Fuera de espacio en el almacenamiento local.
 - Fuera de espacio en el recurso compartido de archivos de red.
 - Se encontraron archivos no válidos.

Nota:

Si un trabajo falla, vuelve a intentarlo en el siguiente intervalo de comprobación, independientemente de si el problema se ha resuelto.

- **Si se encuentra otra actualización antes de instalar una previamente descargada**, la nueva actualización se descarga y, una vez completada correctamente, pasa a ser “Actualización disponible”.
- **Si se descarga una actualización cuando otra está disponible**, la descarga en ejecución se interrumpe y se inicia una nueva descarga. Todos los archivos relacionados con la descarga en curso se eliminan.

Opcional: Cómo comprobar manualmente las actualizaciones disponibles

Las comprobaciones de actualización automatizadas siempre extraen la versión más reciente, pero puede comprobar manualmente si hay actualizaciones.

Para comprobar manualmente si hay una actualización:

1. Inicie sesión en la consola de administración.
2. Haga clic en la ficha **Usuario** y, a continuación, en la acción **Actualizar dispositivo**. La versión más reciente aparece en el campo **Actualizar disco**.

Si ha iniciado sesión en un escritorio como administrador y se muestra una insignia de Actualización:

1. Haga clic en **Iniciar actualización**. La información de descarga se muestra en el campo **Disco de actualización**.
2. Como administrador, puede seleccionar un **disco de actualización** diferente.

Siga los pasos detallados en la sección anterior, [Actualizar el dispositivo](#).

Configuraciones de conectores

May 9, 2024

La primera vez que use el servicio App Layering, planea crear una o más “configuraciones de conectores”. Las configuraciones del conector de App Layering son conjuntos almacenados de credenciales que el dispositivo utiliza para acceder a las ubicaciones del hipervisor o del servidor de Provisioning. Una configuración de conector puede especificar dónde crear una capa o dónde publicar imágenes.

Por qué utilizar configuraciones de conectores

Las configuraciones de conectores permiten que el dispositivo App Layering acceda a las ubicaciones de su entorno para crear capas o publicar imágenes en capas. El uso de una configuración de conector automatiza el proceso de transferencia de archivos y ahorra mucho tiempo.

Puede utilizar una configuración de conector para:

- Cree una capa de aplicación o capa de plataforma, o agregue una versión a una capa del sistema operativo y, si lo quiere, ejecute también un script.
- Publique imágenes en capas en su Hypervisor o servidor de Provisioning y, si lo quiere, ejecute también un script.

Crear capas

La creación de capas es más fácil cuando se utiliza una configuración de conector. La configuración del conector incluye las credenciales para la ubicación en la que planea instalar el software de una capa. Esta configuración del conector incluye una opción de caché de empaquetado, que está habilitada de forma predeterminada para ofrecerle el mejor rendimiento de capas.

Publicar imágenes en capas

Necesita una configuración de conector para cada ubicación en la que publica imágenes en capas. Una vez publicadas, se utilizan imágenes en capas para aprovisionar sistemas para grupos específicos de usuarios.

Requisitos

Para crear una configuración de conector, debe cumplir los siguientes requisitos.

Credenciales

Credenciales de cuenta válidas que el dispositivo puede utilizar para acceder a una ubicación del entorno. Para obtener más información sobre los valores que necesita, seleccione el hipervisor o Provisioning Services más adelante en esta sección.

Acerca de la composición de descargas

Al crear una capa o publicar una imagen en capas, puede usar el *motor de composición* integrado de App Layering para crear capas. El motor de composición se activa seleccionando la opción de

configuración del conector de **composición** de descarga. El `ImportOsLayer.ps1` script se usa al crear una capa de sistema operativo desde cero. Asegúrese de abrir los puertos del firewall necesarios para el [motor de composición](#)

Nota:

Se crea una capa de SO (inicialmente) importando el SO desde una máquina virtual existente. Una vez creada, actualiza la capa del sistema operativo como cualquier otra capa.

Composición de descarga:

- Reduce el tiempo de procesamiento de las tareas de estratificación.
- Permite la creación de imágenes UEFI con particiones vTPM y GPT. Estas funciones son necesarias para las versiones modernas del sistema operativo Windows, como Windows 11.
- Permite la creación de discos VHDX.
- Puede eliminar automáticamente algunos problemas del sistema de archivos con herramientas nativas de Windows

Para crear una capa mediante la composición de descarga:

- **Capa de aplicación, capa de plataforma:** Al crear una capa, elija una configuración de **conector con la composición de descarga** habilitada.
- **Capa de SO:** ejecute un script. Para obtener más información, consulte [Crear capa de SO](#).

Espacio en disco para caché

En todos los hipervisores compatibles, excepto en Azure, el *tamaño predeterminado de la caché de empaquetado* se establece en el nivel inicial recomendado. Permita suficiente espacio en disco para aumentar el tamaño de la caché, si es necesario.

- Crea la capa o imagen como máquina UEFI o Generación 2.
- Utiliza el formato de disco VHDX para el formato BIOS y Generación 1, o para las imágenes UEFI y Generación 2.

Para crear una capa de aplicación o plataforma con Offload Compositing, seleccione una configuración de conectores con **Offload Compositing** habilitada. Para crear una capa de SO, ejecute un script en su lugar. Para obtener más información, consulte [Crear capa de SO](#).

Capas de empaquetado

Cuando se utiliza la **composición de descarga** en la configuración del conector, el empaquetado de una capa comienza cuando se apaga la máquina para su finalización. El empaquetado se realiza au-

tomáticamente. No es necesario que seleccione **Finalizar** manualmente en la consola de administración.

Importante:

Debe ejecutar el script para crear una capa de sistema operativo. También puede compilar el SO en un BIOS o en una máquina de primera generación y, a continuación, agregar una versión a la capa con la opción **de composición de descarga** seleccionada.

Al seleccionar **Descargar composición, elija** UEFI o **Generation 2 para la nueva versión de** capa. Seleccione **VHDX** para el formato del disco. El formato VHDX es compatible con máquinas BIOS (generación 1) y UEFI (generación 2).

Publicar imágenes

Al publicar una imagen, la máquina de publicación genera la imagen en el servidor del hipervisor (Hyper-V, VMware vSphere).

Conectividad

Cuando usas Offload Compositing, se crea una máquina virtual de trabajo temporal en tu entorno, que se denomina motor de composición. El motor de composición requiere conectividad directa con el dispositivo App Layering a través de SSL (puerto 443) e iSCSI (puerto 3260). Asegúrese de que este tráfico esté permitido en su entorno de App Layering. De lo contrario, las tareas creadas desde el dispositivo no se completarán correctamente.

Acerca de “Tamaño de caché de empaquetado” y “Tarifa de selección”

Las configuraciones de conectores para todos los hipervisores, excepto Azure, permiten configurar el espacio para una *caché de empaquetado*. El dispositivo utiliza esta memoria caché en el hipervisor para acelerar el empaquetado de capas.

Tamaño de caché de empaquetado

Recomendamos utilizar el tamaño de inicio de la caché de empaquetado predeterminado para el hipervisor:

- vSphere: 250 GB
- XenServer: 480 GB
- Hyper-V: 200 GB

- Nutanix: 480 GB

Cuantas más capas de aplicaciones cree, mayor será la caché que necesitará. Aumente el [tamaño de la caché de empaquetado](#), si es necesario.

La tasa Hit

La tasa **Hit** es el porcentaje de veces que el dispositivo ha encontrado un disco en la memoria caché. Un valor bajo en este campo indica que la caché no proporciona mucho valor. Aumente el tamaño de la caché para acomodar capas más únicas.

Puede mejorar una tasa baja aumentando el tamaño de la caché de empaquetado. Aumentar el tamaño de la caché permite almacenar más discos en la caché. También aumenta la probabilidad de encontrar un disco para empaquetar en la caché. El resultado es un valor de tasa **hit** más alto.

Ver configuraciones de conectores

La ficha **Conectores** enumera las configuraciones de conectores que ha creado.

Ordenar configuraciones de conectores

De forma predeterminada, las configuraciones del conector se enumeran en orden alfabético por nombre.

Ver detalles de configuración del conector

Cuando se habilita el almacenamiento en caché para una configuración de conector, la ficha **Conectores** muestra el tamaño de la memoria caché para esa configuración.

Para ver los valores de cualquier configuración de conector dada:

1. Haga clic en el botón **Ver detalles** o en el icono de información en la parte derecha de la pantalla. Se muestran los detalles sobre la configuración del conector.

Ver tamaño de caché y tasa Hit

El tamaño de caché de paquetes y la tasa **Hit** se muestran cuando el tamaño de la memoria caché de paquetes se establece en un valor mayor que cero (0).








Agregar una configuración de conector

En esta sección se explica cómo agregar y administrar una configuración de conectores en la ficha **Conectores**.

Una configuración de conector acelera el proceso de creación de una capa o plantilla de imagen. Si necesita uno para acceder a una ubicación específica, puede crear uno seleccionando **Agregar configuración de conectores** en la ficha **Conectores**. A partir de ahí, utilice los pasos detallados más adelante en esta sección.

Para agregar una configuración de conector, siga estos pasos:

1. Acceda a la consola de administración y seleccione **Conectores** para ver las configuraciones de los conectores, si ha creado alguna.
2. Haga clic en **Agregar configuración de conector** en la barra de acciones. Se abre un cuadro de diálogo en el que puede seleccionar el tipo de configuración del conector que quiere crear.
3. Seleccione el tipo de conector en el menú desplegable.
4. Complete los campos de la página Configuración del conector.
5. Haga clic en el botón **Probar** para comprobar que el conector puede acceder a la ubicación especificada mediante las credenciales proporcionadas.
6. Haga clic en **Guardar**. La nueva configuración del conector aparece en la ficha **Conector**.

Name	Platform	Cache Size	Cache Hit Rate
 BIG Cache	VMware vSphere	2147483647 GB	<input type="text"/>
 ESXP14 Slow	Citrix MCS for vSphere		
 Fitz App Layering Dev	Azure RDSH		
 SSDESXP13	VMware vSphere	200 GB	<div style="width: 100%;"><div style="width: 100%;"></div></div>
 UD-Hyperv2	Microsoft Hyper-V		
 vcenter6 - QA	VMware vSphere		
 XenServer2	XenServer		

Modificar una configuración de conector

Para modificar una configuración de conector:

1. Acceda a la consola de administración y seleccione **Conectores**.
2. Seleccione el conector y haga clic en **Modificar** en el panel de acciones o en el lado derecho de la pantalla. Se muestra la configuración del conector.
3. Actualice la configuración, según sea necesario.
4. Haga clic en el botón **Probar** para comprobar que el conector puede acceder a la ubicación especificada mediante las credenciales proporcionadas.
5. Haga clic en **Guardar**. Se actualiza la configuración del conector.

Aumenta el tamaño de caché y la tasa Hit

Para mejorar la utilidad de la memoria caché y, por lo tanto, aumentar la tasa **hit** mediante la edición del tamaño de la caché de paquetes:

1. Seleccione el conector y haga clic en **Modificar** en el panel de acciones o en el lado derecho de la pantalla.
2. Desplácese hasta **Tamaño de caché de disco de capa en GB** e introduzca la cantidad de espacio que puede ocupar la caché
3. Haga clic en el botón **Probar** para comprobar que el conector puede acceder a la ubicación especificada mediante las credenciales proporcionadas.
4. Haga clic en **Guardar**. Se actualiza la configuración del conector.

Continúe ajustando el tamaño de la caché hasta que logre el rendimiento de capas que está buscando.

Inhabilitar o volver a habilitar el almacenamiento en caché

El almacenamiento en caché está *habilitado* y se establece en un tamaño inicial recomendado de forma predeterminada. Le recomendamos encarecidamente que utilice el almacenamiento en caché.

Si inhabilita el almacenamiento en caché para una configuración de conector, establezca el tamaño de caché en cero (0). Puede volver a habilitarla aumentando el tamaño de la caché de empaquetado.

Eliminar una configuración de conector

Para eliminar una configuración de conector:

1. En la consola de administración, seleccione **Conectores**.
2. Asegúrese de que la configuración del conector no está en uso.
3. Haga clic en **Eliminar** en la barra de acciones o en el lado derecho de la pantalla.
4. En la ventana emergente que se abre, selecciona **Eliminar**. Se elimina la configuración del conector.

La ficha **Conectores** tarda unos minutos en actualizarse después de que otro administrador elimine una configuración de conector.

Mensajes al eliminar configuraciones de conectores

Si se está utilizando una configuración de conector cuando intenta eliminarla, recibirá un mensaje similar al del siguiente ejemplo:

“**Error de validación: no se puede eliminar la configuración del conector ‘Citrix Provisioning - ConnectorExample’ mientras está en uso.** Si recibe este mensaje de error, quite la configuración del conector de la plantilla de capa o imagen en la que aún esté en uso. A continuación, borre la configuración.”

Implementaciones de Azure

June 27, 2024

Al crear capas o publicar imágenes en un entorno de Azure, utilice la configuración del conector **Azure Deployments** o **Machine Creation for Azure Deployments**. En este artículo se describen los parámetros de configuración del conector. Para obtener más información sobre las configuraciones de conectores y cómo agregar otras nuevas, consulte [Configuraciones de conectores](#).

Nota:

Azure Deployments también es compatible con Azure Government.

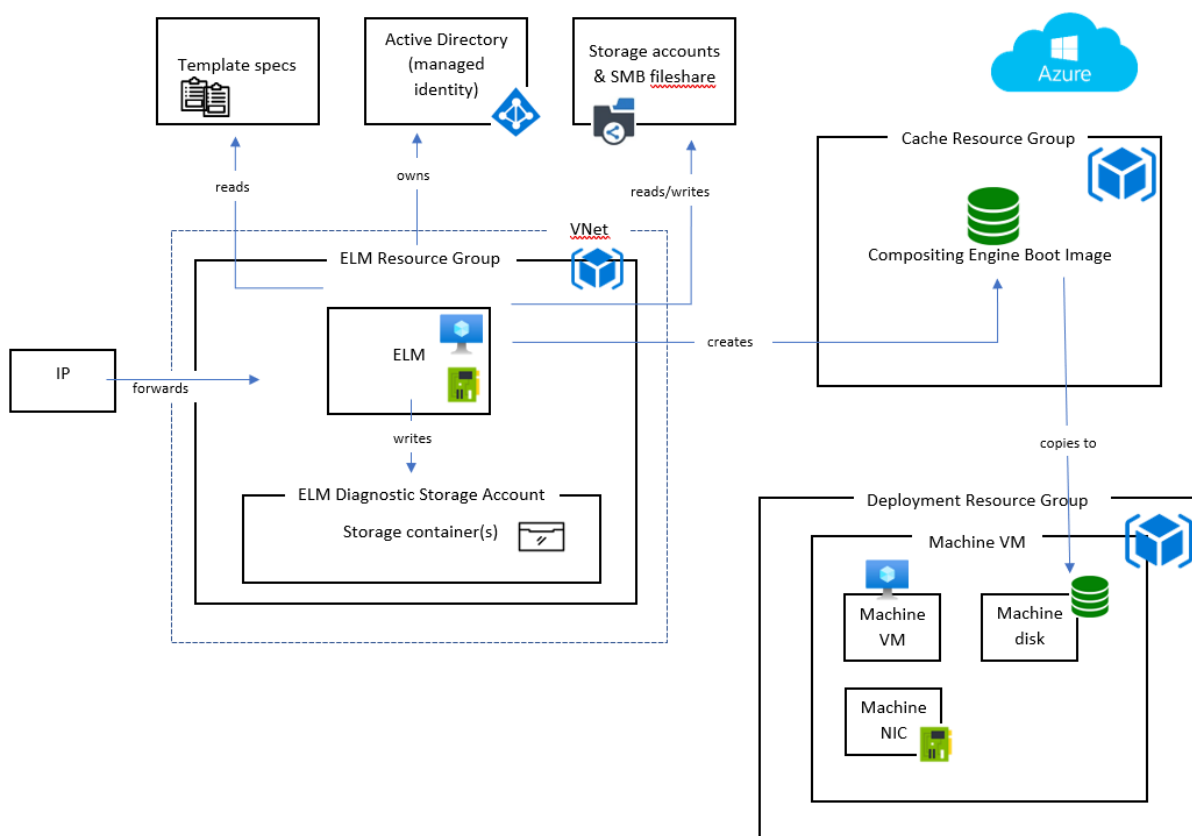
Introducción

Las implementaciones de Azure en App Layering se refieren a la creación de implementaciones de Azure mediante plantillas de Azure Resource Manager (ARM). Las plantillas ARM son documentos JSON específicos de Azure que definen la infraestructura y la configuración como código. Para obtener más información sobre las plantillas ARM, consulte la documentación de Azure [aquí](#).

Todos los recursos de Azure creados por el conector App Layering Azure Deployments se crean mediante la implementación de una plantilla ARM especificada por el usuario. Estas plantillas permiten al administrador personalizar ampliamente los recursos que se crean y la forma en que se configuran.

Especificaciones de la plantilla de Azure

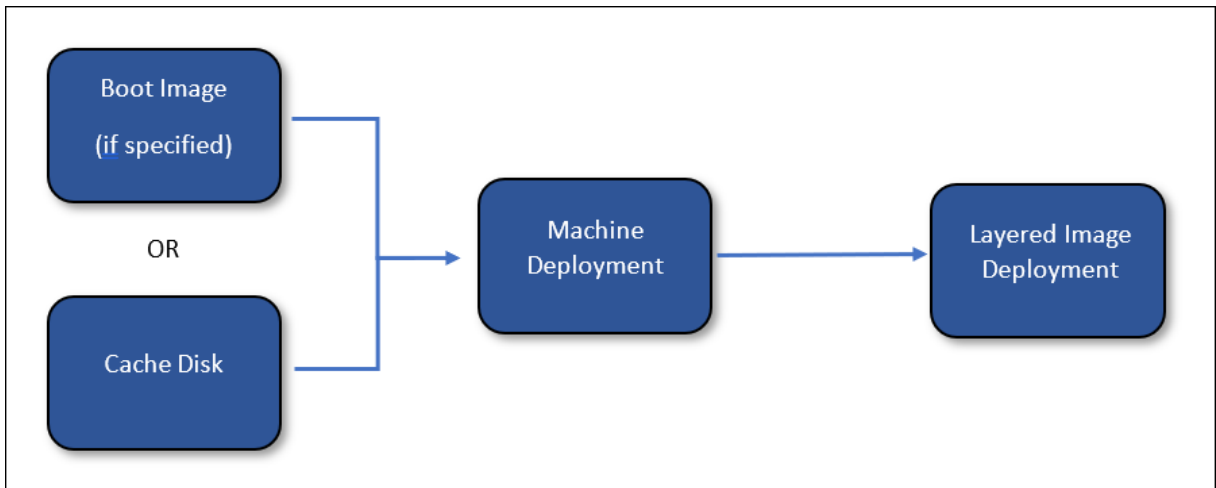
Las [especificaciones de plantillas de Azure](#) son un tipo de recurso de Azure que almacena y versiona una plantilla ARM para su uso posterior en una implementación de plantillas ARM. Debe especificar entre dos y cuatro especificaciones de plantilla para cada configuración de conector de Azure Deployments. Cada tipo de implementación de un conector de Azure Deployments requiere la versión correspondiente de una especificación de plantilla. Las implementaciones de **máquina** y **disco de caché** son obligatorias, pero las implementaciones de **imagen de arranque** e **imagen en capas** son opcionales.



Tipos de implementación

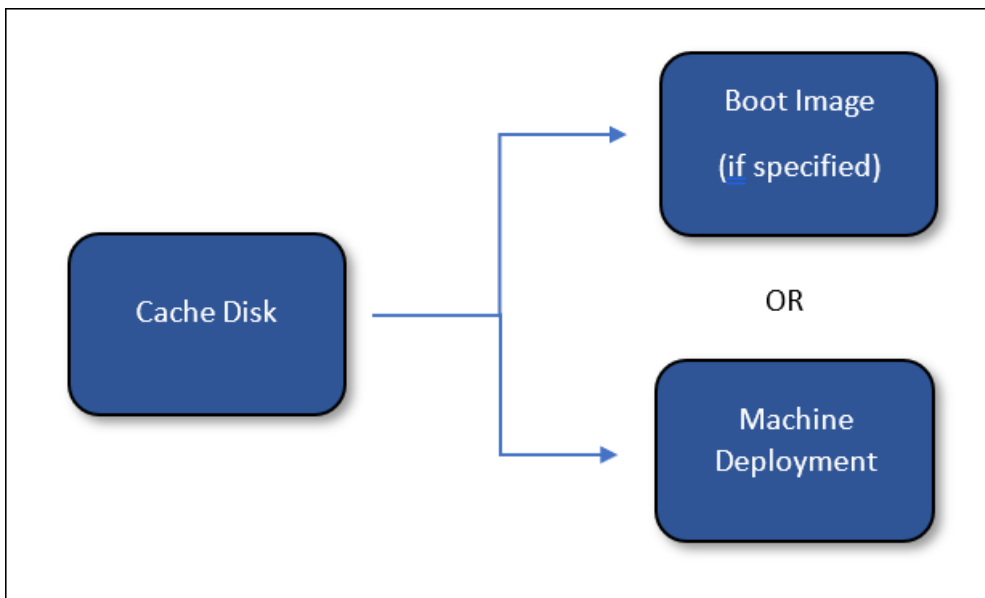
Hay cuatro tipos de implementación, cada uno de los cuales requiere su especificación de plantilla. Los tipos de implementación difieren en el tipo de recursos que crean, las entradas que reciben y las salidas que producen para anular el comportamiento predeterminado. Para obtener más información sobre estos conceptos, consulte [Creación de plantillas ARM](#).

Máquina La implementación **de máquinas** crea una máquina virtual (VM). Las máquinas virtuales creadas por implementaciones de **máquinas** pueden componer imágenes en capas y capas de paquetes. Si no se especifica la implementación opcional de **imágenes en capas**, el resultado final de la publicación de una imagen es una máquina virtual. En este caso, la máquina virtual se puede usar tal cual o como imagen maestra de Machine Creation Services (MCS).



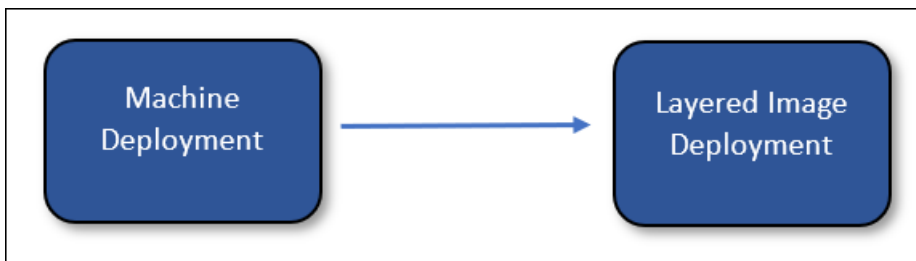
Si se especifica una implementación de la **Imagen en capas**, los recursos creados por la implementación de la **Máquina** se eliminan una vez que se haya completado la implementación de la **Imagen en capas**. De lo contrario, App Layering no elimina los recursos (a menos que falle la implementación).

Disco de caché La implementación del **disco caché** crea un disco administrado por Azure. Este disco se utiliza para contener la imagen de arranque de Compositing Engine. El dispositivo App Layering carga el contenido en el disco una vez creado.



Si se especifica una implementación de la **Imagen de arranque**, los recursos creados por la implementación del **Disco de caché** se eliminan una vez finalizada la implementación de la **Imagen de arranque**. De lo contrario, App Layering elimina los recursos durante la limpieza de la memoria caché.

Imagen en capas (opcional) La implementación de **imágenes en capas** es un tipo de implementación opcional. Los recursos resultantes son el resultado final de publicar una imagen en capas. No es necesario crear ningún tipo de recurso en particular. La implementación de **imágenes en capas** se puede utilizar para producir una [imagen de galería de cómputos](#), un disco administrado o cualquier otro tipo de recurso.



App Layering no elimina los recursos creados por la implementación de imágenes en capas (a menos que se produzca un error en la implementación).

Imagen de arranque (opcional) La implementación de **de Boot Image** es un tipo de implementación opcional. Los recursos resultantes se utilizan para crear los discos del sistema operativo de las máquinas virtuales creadas por las implementaciones de la **Máquina**. No es necesario crear ningún tipo de recurso en particular, sin embargo, debe crear un recurso que pueda usarse para crear un disco de sistema operativo para una máquina virtual. Esta implementación se puede usar para producir una [imagen de la galería de cómputos](#) o cualquier otro tipo de recurso que pueda usarse como fuente de un disco.



App Layering elimina los recursos creados por la implementación de la imagen de arranque durante la limpieza de la memoria caché.

Identidad de máquina del dispositivo App Layering

Hay dos formas de conectarse mediante Azure Deployments: como una identidad gestionada o como una aplicación registrada (similar al conector de Azure heredado). Si bien el uso de una identidad gestionada es una forma cómoda de conceder derechos al dispositivo, el uso de las credenciales de registro de la aplicación permite a Azure Deployments acceder a los recursos de todos los inquilinos y configurarse en dispositivos que no residen en Azure.

Identidad gestionada

Con Azure Deployments, ahora puede autenticarse en Azure con la [identidad gestionada](#) asignada al dispositivo App Layering en Azure.

Dado que se debe [asignar una identidad gestionada](#), este método solo se admite en un dispositivo de App Layering implementado en Azure.

Credenciales de registro

Para autenticarse mediante sus credenciales de registro, la configuración del conector de Azure Deployments requiere la siguiente información:

- **Entorno de Azure:** El entorno que se utiliza, ya sea Azure Public Cloud o Azure Government.
- **ID de arrendatario:** Instancia de Azure Active Directory, este GUID identifica la instancia dedicada de Azure Active Directory (AD) de su organización.
- **ID de cliente:** Identificador del registro de aplicaciones, que su organización ha creado para App Layering.
- **Secreto de cliente:** La contraseña del **ID de cliente** que está utilizando. Si ha olvidado el secreto del cliente, puede crear uno nuevo.

Nota:

Los secretos de cliente se asocian de forma lógica a los inquilinos de Azure, por lo que cada vez que utilice un nuevo ID de arrendatario, deberá utilizar un nuevo **secreto de cliente**.

Agregar una configuración de conector

Consulte las siguientes descripciones para obtener información sobre cada campo de la pantalla de configuración del conector.

Valores predeterminados (opcional)

Los valores predeterminados son opcionales y se pueden usar para aplicar **etiquetas** y **datos personalizados** a todos los tipos de implementación en la configuración del conector. Los datos especificados en los valores predeterminados se combinan con los datos especificados en los campos correspondientes de cada tipo de implementación.

Implementaciones

Cada tipo de implementación contiene los siguientes campos.

Plantilla La especificación de plantilla utilizada para la implementación. El usuario crea y administra las especificaciones de la plantilla en Azure. La identidad gestionada o las credenciales de registro del dispositivo deben tener permiso de lectura en el grupo de recursos que contiene la especificación de la plantilla.

Versión La versión de la especificación de plantilla que se utilizará para la implementación. La versión más reciente se selecciona de forma predeterminada cuando se cambia la selección de **Plantillas**.

Grupo de recursos El grupo de recursos de Azure en el que se va a implementar. Todos los recursos creados por la implementación se crean en este grupo de recursos.

La identidad gestionada o las credenciales de registro del dispositivo deben tener permiso para:

- Implemente plantillas en el grupo de recursos
- Crea cada tipo de recurso en la plantilla
- Eliminar cada tipo de recurso de la plantilla

Al asignar la [función de colaborador general](#) a la identidad gestionada o a las credenciales de registro del grupo de recursos, se otorgan los permisos necesarios. En su lugar, se pueden especificar permisos o funciones más detallados, pero los permisos necesarios dependen de los recursos especificados en la plantilla.

Nota:

La identidad gestionada del dispositivo debe tener permiso para conectar un dispositivo a la red virtual especificada para la máquina virtual creada por la implementación de la **Máquina**. Si la red virtual no se encuentra en ninguno de los grupos de recursos especificados para las implementaciones, las funciones asignadas a la identidad gestionada o a las credenciales de registro de esos grupos de recursos no se aplicarán a la red virtual y se deberá asignar una función directamente a la red virtual.

Etiquetas (avanzadas) Las etiquetas que se aplicarán al artefacto de implementación de Azure creado por una implementación. Puede incluir datos del parámetro de entrada (consulte [Creación de plantillas ARM](#)). Para ello, coloca la ruta JSON del campo al que quieres hacer referencia entre llaves. Por ejemplo, { `context.user` } se evalúa con el nombre del usuario de App Layering que creó la tarea que provocó la implementación. Esto funciona tanto para el nombre de la etiqueta como para los campos de valor de la etiqueta. Si quieres usar llaves literales en tus etiquetas, puedes evitarlas doblándolas. Por ejemplo, se evalúa como `{}`.

Importante:

Estas etiquetas *solo* se aplican al propio recurso de implementación. No se aplican a los recursos creados por la implementación. Para aplicar etiquetas a los recursos creados, especifique esas etiquetas en la plantilla ARM.

Datos personalizados (avanzados) Datos arbitrarios especificados en formato JSON. Se puede hacer referencia a estos datos en la plantilla ARM asociada a la implementación. Se accede a los datos mediante el objeto `context.config.custom` del parámetro de entrada. Consulte [Creación de plantillas ARM](#) para obtener más información.

Consideraciones

- Se requiere conectividad de red entre el dispositivo App Layering y las máquinas virtuales creadas por la implementación de la máquina.
 - Desde las máquinas virtuales creadas por la implementación de la máquina, el tráfico IP debe poder enrutarse a la dirección IP del dispositivo App Layering en los puertos 443 (HTTPS) y 3260 (iSCSI). Además, el tráfico del dispositivo App Layering debe poder enrutarse a la dirección IP de estas máquinas virtuales (creada por el despliegue de la máquina) en el puerto 443 (HTTPS).
 - Los dispositivos de App Layering implementados localmente deben estar conectados a la red virtual de Azure especificada para las máquinas virtuales creadas por la implementación de la máquina. Puede conectar redes virtuales locales a Azure a través de Azure [ExpressRoute y [Azure VPN](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction)](<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction>)Gateway.
- Los conectores Legacy Azure están en desuso, pero seguirán estando disponibles durante un tiempo limitado. No hay ninguna ruta de actualización ni migración desde ningún conector de Azure antiguo a los nuevos tipos de conectores de Azure Deployments. Para obtener más información, consulte [Citrix App Layering en Azure](#).

Creación de plantillas ARM

May 9, 2024

Esta sección está destinada a usuarios familiarizados con las plantillas ARM. Proporciona información detallada sobre la creación de plantillas para el conector de Azure Deployments de App Layering.

Para obtener información general sobre la creación de plantillas ARM, consulte la [documentación de Microsoft](#).

Entrada

A cada tipo de implementación se le pasa un parámetro, un objeto denominado `al`. Este objeto tiene dos propiedades, `input` y `context`. La propiedad `input` es un objeto específico de cada tipo de implementación y sus propiedades cambian según el tipo de implementación. La propiedad `context` es la misma para todos los tipos de implementación. Contiene datos sobre la tarea, el elemento (plantilla de capa o imagen) y la configuración del conector de App Layering asociados a la implementación actual. Para obtener información detallada sobre el objeto de parámetro, consulte el [parámetro de plantilla de Azure Deployments](#).

Cada plantilla debe declarar el parámetro `al` en su sección de parámetros, de la siguiente manera:

```
1 {
2
3     ...
4     "parameters": {
5
6         "al": {
7
8             "type": "object"
9         }
10    }
11  },
12  ...
13 }
14
15
16 <!--NeedCopy-->
```

Una plantilla puede declarar más parámetros, pero todos los parámetros deben tener valores predeterminados. De lo contrario, App Layering no les proporciona valor. Esto puede resultar útil para usar funciones que solo se pueden usar en la sección de valores predeterminados de un parámetro, por ejemplo `utcNow`.

Resultado

Todas las plantillas ARM pueden tener salidas. Con el conector de Azure Deployments, las salidas de las plantillas se pueden utilizar para pasar información a la siguiente implementación. También se pueden usar para anular algunos comportamientos predeterminados.

Los resultados de una implementación se pasan a la siguiente implementación mediante la propiedad `input` del `al` [parámetro template](#).

Por ejemplo, cuando una implementación de un **disco de caché** tiene los siguientes resultados:

```
1 {
2
3   ...
4   "outputs": {
5
6     "generation": {
7
8       "type": "string",
9       "value": "[variables('generation')]"
10    }
11  ,
12    "name": {
13
14      "type": "string",
15      "value": "[variables('name')]"
16    }
17  ,
18  }
19
20  ...
21 }
22
23 <!--NeedCopy-->
```

La implementación **de Boot Image** recibe esta entrada:

```
1 {
2
3   "input":
4   {
5
6     "type": "BootImage",
7     "source": {
8
9       "generation": "V2",
10      "name": "MyCoolDiskName"
11    }
12  }
13
14  ,
15  "context": {
16
17    ...
18  }
19
20 }
21
22 <!--NeedCopy-->
```

Observe que la propiedad `source` del objeto `input` tiene una propiedad para cada salida especificada en la plantilla de implementación del **Disco de caché**. Los orígenes de cada salida dependen

del tipo de implementación.

Detalles del tipo de implementación

Cada tipo de implementación tiene un conjunto diferente de entradas y salidas que pueden cambiar el comportamiento de la operación de App Layering. Estos detalles específicos de la implementación se describen en esta sección.

Para ver ejemplos del mundo real que utilizan todos estos conceptos, consulte [Plantillas para principiantes](#).

Disco de caché

La implementación del disco de caché debe crear un recurso de disco administrado. Si lo desea, puede crear otros recursos además del disco. El dispositivo App Layering debe tener permiso para escribir en el disco mediante un token SAS (generado por el dispositivo). Una vez creada, se carga en el disco una imagen de arranque que contiene el motor de composición de App Layering.

Requisitos de disco de caché

- Debe crear un recurso de disco administrado
- `createOption` del disco administrado debe estar configurado en `"Upload"`
- `uploadSizeBytes` del disco administrado debe estar configurado en el valor `uploadSize` especificado en la entrada, como `"[parameters('al').input.uploadSize]"`
- El dispositivo App Layering debe poder escribir en el disco administrado mediante un token SAS.

```
1 {
2
3     ...
4     "resources": [
5         {
6
7             "type": "Microsoft.Compute/disks",
8             ...
9             "properties": {
10
11                 ...
12                 "creationData": {
13
14                     "createOption": "Upload",
15                     "uploadSizeBytes": "[parameters('al').input.
16                                     uploadSize]"
17                 }
18             }
19         }
20     ]
21 }
```

```
18         ...
19     }
20
21     }
22
23 ]
24 ...
25 }
26
27 <!--NeedCopy-->
```

Entrada de disco de caché El [objeto de entrada](#) incluye las propiedades `size` y `uploadSize`. Este objeto no incluye los resultados de otra implementación.

Salida de disco de caché El resultado de la implementación se pasa a la implementación de **Boot Image** si se especifica alguna. De lo contrario, se pasa a la implementación de la **Máquina**.

Se puede especificar una salida denominada `diskId` para indicar explícitamente a App Layering qué disco usar. Si no se especifica ninguna salida de `diskId`, App Layering agrega una automáticamente y la configura en el ID de recurso del primer recurso de disco administrado creado por la implementación. El disco especificado por `diskId` tiene cargada la imagen de arranque del motor de composición de App Layering.

Imagen de arranque

Esta implementación crea un recurso a partir del disco administrado creado por la implementación del **Disco de caché**. No hay requisitos estrictos en cuanto al tipo de recursos que se crean. Sin embargo, debe crear un recurso que pueda usarse como fuente de un disco del sistema operativo al crear una máquina virtual, como una versión de imagen de una galería de cómputos.

Requisitos del disco de imagen de arranque

- Debe crear un recurso que pueda usarse para crear el disco del sistema operativo de una máquina virtual con el mismo contenido que el disco con el ID ingresado como entrada.

A modo de ejemplo, una versión de imagen de una galería de cómputos que utiliza la entrada `diskId` como origen:

```
1 {
2
3     ...
4     "resources": [
5         {
6
```

```
7     "type": "Microsoft.Compute/galleries/images/versions",
8     ...
9     "properties": {
10    ...
11    "storageProfile": {
12    "osDiskImage": {
13    "source": {
14    "id": "[parameters('al').input.source.
15    diskId]"
16    }
17    }
18    }
19    }
20    }
21    }
22    }
23    }
24    }
25    ...
26    }
27    }
28    }
29    ]
30    ...
31    }
32    }
33
34 <!--NeedCopy-->
```

Entrada de imagen de arranque El [objeto de entrada](#) incluye la propiedad `source`. `source` representa las salidas de la implementación del **Disco de caché**, con una propiedad para cada salida especificada. Utilice la propiedad `diskId` para el origen del recurso que se está creando.

Salida de imagen de arranque El resultado de la implementación de la **imagen de arranque** se pasa a la implementación de la **Máquina**. No hay salidas especiales ni obligatorias. Sin embargo, debes incluir los datos necesarios para crear una máquina virtual a partir del recurso creado, como un identificador de recurso.

Máquina

La implementación **de la máquina** debe crear un recurso de máquina virtual. La máquina virtual debe estar conectada a una red en la que pueda llegar al dispositivo App Layering y viceversa, según [las conexiones internas de los puertos Firewall para la máquina de composición](#).

Importante:

No conecte el disco creado por la implementación del **disco de caché** a la máquina virtual. El **disco de caché** es un recurso compartido y se considera de solo lectura. Cree una copia del disco y adjúntela en su lugar cuando no utilice la implementación de la **Imagen de arranque**.

Requisitos de máquina

- Debe crear un recurso de máquina virtual
- La máquina virtual debe estar conectada a una red que permita la comunicación hacia y desde el dispositivo App Layering.
- El disco del sistema operativo de la máquina virtual debe crearse utilizando el recurso **de imagen de arranque** o **disco de caché** como fuente
- El tamaño del disco del sistema operativo de la máquina virtual debe configurarse en `"[parameters('al').input.disk.size]"`
- La propiedad `userData` de la máquina virtual debe estar configurada en `"[parameters('al').input.vm.userData]"`

```
1 {
2
3     ...
4     "resources": [
5         {
6
7             "type": "Microsoft.Compute/disks",
8             "name": "[variables('diskName')]",
9             ...
10            "properties": {
11
12                ...
13                "creationData": {
14
15                    "createOption": "Copy",
16                    "sourceResourceId": "[parameters('al').input.disk.
17                        image.diskId]"
18                }
19            },
20            "diskSizeGB": "[parameters('al').input.disk.size]",
21            ...
22        }
23    ],
24    {
25
26
27        "type": "Microsoft.Compute/virtualMachines",
28        ...
29        "dependsOn": [
```

```

30         "[resourceId('Microsoft.Compute/disks', variables('
31             diskName'))]"
32     ],
33     ...
34     "properties": {
35         ...
36         "storageProfile": {
37             ...
38             "osDisk": {
39                 ...
40                 "createOption": "Attach",
41                 "managedDisk": {
42                     ...
43                     "id": "[resourceId('Microsoft.Compute/disks
44                         ', variables('diskName'))]"
45                 }
46             }
47         }
48     },
49     "dataDisks": []
50 }
51 ,
52     ...
53     "userData": "[parameters('al').input.vm.userData]"
54     ...
55 }
56 }
57 ]
58 ...
59 }
60 }
61 }
62 }
63 <!--NeedCopy-->

```

Entrada de máquina El [objeto de entrada](#) incluye las propiedades `disk` y `vm`.

La propiedad `disk.image` contiene el resultado de la implementación de la **Imagen de arranque**, si se especificó alguna. De lo contrario, contiene el resultado de la implementación del **Disco de caché**. La propiedad `disk.size` contiene el tamaño del disco en GB.

La propiedad `vm.userData` contiene los datos de usuario que se deben asignar a la máquina virtual creada.

Salida de la máquina El resultado de la implementación de la **máquina** se pasa a la implementación de **imágenes en capas** si se especifica alguna. Si utiliza una implementación de **imágenes en capas**, debe incluir el ID de la máquina virtual o el disco del sistema operativo en la

salida para que la implementación de **imágenes en capas** pueda hacer referencia a ella.

Se puede especificar una salida denominada `machineId` para indicar explícitamente a App Layering qué máquina virtual usar. Si no se especifica ninguna salida de `machineId`, App Layering agrega una automáticamente y la configura en el ID de recurso del primer recurso de máquina virtual creado por la implementación.

Se puede especificar una salida denominada `ipAddress` para indicar explícitamente a App Layering qué dirección IP usar para comunicarse con la máquina. Si no se especifica ninguna salida de `ipAddress`, App Layering utiliza la dirección privada principal de la tarjeta de red principal conectada al recurso de la máquina virtual.

Se puede especificar una salida denominada `message` para proporcionar un mensaje que se agregue al estado final de una tarea de publicación de imágenes y al estado de acción requerida de una tarea de creación de capas en la interfaz de usuario de App Layering. Este mensaje solo se usa en el estado final de la tarea de publicación de imágenes si no se especifica una implementación de la **imagen en capas**.

- La [plantilla Machine Starter](#) establece el parámetro de salida `message` en un enlace a la máquina en el portal de Azure.

Imagen en capas

La implementación de la **Imagen en capas** crea un recurso a partir de la máquina virtual u otros recursos creados por la implementación de la **Máquina**. No hay requisitos estrictos en cuanto al tipo de recursos que se crean. Sin embargo, crea un recurso que se puede usar como entrada para un servicio de aprovisionamiento, como Machine Creation Services (MCS). Un recurso de imágenes de galería de cómputos es un buen ejemplo.

Requisitos de disco de imagen en capas

- Crea un recurso que puede usar un servicio de aprovisionamiento para crear máquinas virtuales.

A modo de ejemplo, el siguiente bloque de código crea una versión de imagen de la galería de cómputos con la entrada `diskId` como origen. Esto supone que la implementación de la **Máquina** incluyó una salida denominada `diskId` que se establece con el ID del disco del sistema operativo de la máquina:

```
1 {
2
3   ...
4   "resources": [
5     {
```

```
6
7     "type": "Microsoft.Compute/galleries/images",
8     "name": "[format('{
9 0 }
10 /{
11 1 }
12 ', variables('galleryName'), variables('name'))]",
13     ...
14     "resources": [
15         {
16
17             "type": "versions",
18             ...
19             "dependsOn": [
20                 "[resourceId('Microsoft.Compute/galleries/
21                     images', variables('galleryName'), variables
22                     ('name'))]"
23             ],
24             ...
25             "properties": {
26                 ...
27                 "storageProfile": {
28                     "osDiskImage": {
29                         "source": {
30                             "id": "[parameters('al').input.
31                                 source.diskId]"
32                             }
33                         }
34                     }
35                 }
36             }
37             ...
38             ...
39             ...
40             ...
41             ...
42             ...
43         }
44     ]
45 }
46
47 ],
48 ...
49 }
50
51 <!--NeedCopy-->
```

Entrada de imagen en capas El **objeto de entrada** incluye las propiedades `source` y `diskName`. `source` representa las salidas de la implementación de la **Máquina**, con una propiedad para cada

salida especificada. La propiedad `diskName` es el nombre del disco especificado en la plantilla de imagen de App Layering.

Salida de imagen en capas El resultado de la implementación no se pasa a ninguna otra implementación. Sin embargo, se puede especificar una salida denominada `message` para proporcionar un mensaje que se adjunte al estado final de una tarea de publicación de imágenes en la interfaz de usuario de App Layering.

Plantillas de inicio

May 9, 2024

Esta sección contiene un conjunto completo de plantillas ARM que se pueden usar con el conector de Azure Deployments. Estas plantillas se pueden utilizar tal cual o se pueden modificar para satisfacer necesidades específicas.

Cada recurso creado por estas plantillas se etiqueta con el mismo conjunto de etiquetas. Estas etiquetas incluyen información útil sobre el contexto de la implementación, como el nombre del usuario que inició la tarea y el comentario que introdujo.

Las plantillas utilizan ampliamente los datos personalizados en la [configuración del conector](#). Los datos personalizados permiten al usuario definir parámetros comunes como `locationvmSize` `generation`, y otros parámetros sin necesidad de modificar la plantilla.

En la siguiente tabla se enumeran todas las propiedades de datos personalizadas que utilizan estas plantillas. Especifica qué plantillas se aplican a cada propiedad y si la propiedad es obligatoria.

R = Obligatorio, O = Opcional, - = No se utiliza

Nombre	Tipo	Descripción	Valor predeterminado	Disco de caché	Imagen de arranque	Máquina	Imagen en capas
Ubicación	cadena	La región donde se crean los recursos.	La misma región que el grupo de recursos de destino.	O	O	O	O

App Layering

Nombre	Tipo	Descripción	Valor predeter- minado	Disco de caché	Imagen de arranque	Máquina	Imagen en capas
gallery	cadena	El nombre de la galería de procesamiento en la que se crean las imágenes. La galería debe estar en el grupo de recursos de destino.	-	-	R	-	R
storageSku	cadena	El nombre del SKU que se utilizará para los discos gestionados.	“Standard-SSD_LRS”	0	-	0	-
generation	cadena	La generación de máquinas virtuales.	“V2”	-	0	0	0

Nombre	Tipo	Descripción	Valor predeter- minado	Disco de caché	Imagen de arranque	Máquina	Imagen en capas
Lanzamiento confiable	booleano	para habilitar Trusted Launch, lo contrario. Debe ser el mismo valor para todos los tipos de imple- mentación.	false	0	0	0	0

Nombre	Tipo	Descripción	Valor predeter- minado	Disco de caché	Imagen de arranque	Máquina	Imagen en capas
diskAccessIdcadena		El ID de recurso del acceso al disco utilizado al cargar el contenido del disco. Si se especifica, el disco se crea con el acceso a la red pública desactivado. Para obtener más información, consulte la documentación de Azure .	null	0	-	-	-
vmSize	cadena	El tamaño de la máquina virtual que se va a crear.	“Standard_D2s_v3”	-	-	0	-

Nombre	Tipo	Descripción	Valor predeter- minado	Disco de caché	Imagen de arranque	Máquina	Imagen en capas
licenseType	cadena	El tipo de licencia local que se aplicará a las máquinas virtuales creadas.	null	-	-	0	-
subnetId	cadena	El ID del recurso de la subred a la que se debe conectar la tarjeta de red de la máquina virtual.	-	-	-	R	-
Recuento de réplicas	number	El número predeterminado de réplicas por región de la versión de la imagen de la galería	1	-	-	-	0

Nombre	Tipo	Descripción	Valor predeter- minado	Disco de caché	Imagen de arranque	Máquina	Imagen en capas
Regiones objetivo	matriz	Las regiones de destino de la versión de la imagen de la galería. Se especifica como una matriz de cadenas de nombres de regiones u objetos TargetRegion . La matriz debe contener la región del disco de origen (que se especifica en los location datos personalizados).	La región especificada por los location datos personalizados	-	-	-	0

Nombre	Tipo	Descripción	Valor predeter- minado	Disco de caché	Imagen de arranque	Máquina	Imagen en capas
Publicar como	cadena o matriz	El tipo de recurso (s) en el que publicar imágenes. Se especifica como una matriz o cadena que consta de «Gallery- Image» y/o «Man- aged- Disk»	[“gallery- Image”]	-	-	-	0

Ejemplo de datos personalizados:

```

1 {
2
3   "gallery": "MyGallery",
4   "subnetId": "/subscriptions/ab3d1259-f5a9-407f-bbdd-bfd5701e2e94/
   resourceGroups/PDGPB/providers/Microsoft.Network/
   virtualNetworks/MyVnet/subnets/mysubnet"
5 }
6
7 <!--NeedCopy-->

```

Otro ejemplo de datos personalizados:

```

1 {
2
3   "location": "eastus",
4   "gallery": "MyGallery",
5   "storageSku": "Premium_LRS",
6   "trustedLaunch": true,
7   "diskAccessId": "/subscriptions/ab3d1259-f5a9-407f-bbdd-
   bfd5701e2e94/resourceGroups/MyResourceGroup/providers/Microsoft.
   Compute/diskAccesses/MyDiskAccess",

```

```

8   "vmSize": "Standard_D4s_v3",
9   "subnetId": "/subscriptions/ab3d1259-f5a9-407f-bbdd-bfd5701e2e94/
    resourceGroups/MyResourceGroup/providers/Microsoft.Network/
    virtualNetworks/MyVnet/subnets/mysubnet",
10  "replicaCount": 2,
11  "targetRegions": [
12    "eastus",
13    {
14
15      "name": "eastus2",
16      "regionalReplicaCount": 5,
17      "storageAccountType": "Premium_LRS"
18    }
19  ,
20    "westus"
21  ]
22 }
23
24 <!--NeedCopy-->

```

Disco de caché

Crea un disco administrado.

Datos personalizados del disco de caché

Nombre	Tipo	Descripción	Valor predeterminado	Si son necesarias
Ubicación	cadena	La región en la que se crean los recursos.	La misma región que el grupo de recursos de destino	no
storageSku	cadena	El nombre del SKU que se va a utilizar.	“Standard-SSD_LRS”	no

Nombre	Tipo	Descripción	Valor predeterminado	Si son necesarias
Lanzamiento confiable	booleano	true para habilitar Trusted Launch, false de lo contrario. Debe ser el mismo valor para todos los tipos de implementación.	false	no
diskAccessId	cadena	El ID de recurso del acceso al disco que se utilizará al cargar el contenido del disco. Si se especifica, el disco se crea con el acceso a la red pública desactivado.	null	no

Plantilla de disco de caché

- 1.1.0.0 - Se ha añadido soporte para Trusted Launch
- 1.0.0.0 - Versión inicial

```
1 {
2
3   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/
4     deploymentTemplate.json#",
5   "contentVersion": "1.1.0.0",
6   "parameters": {
7     "al": {
8
9       "type": "object"
10    }
11  }
12  },
13
```

```
14     "variables": {
15
16         "custom": "[parameters('al').context.config.custom]",
17         "location": "[if(contains(variables('custom'), 'location'),
18             variables('custom').location, resourceGroup().location)]",
19         "name": "[concat(parameters('al').context.item.name, '-',
20             parameters('al').context.item.id)]",
21         "tags": {
22             "alTaskId": "[parameters('al').context.taskId]",
23             "alUser": "[parameters('al').context.user]",
24             "alComment": "[parameters('al').context.comment]",
25             "alItemType": "[parameters('al').context.item.type]",
26             "alItemId": "[parameters('al').context.item.id]",
27             "alItemName": "[parameters('al').context.item.name]",
28             "alItemVersion": "[parameters('al').context.item.version.
29                 name]",
30             "alConfigId": "[parameters('al').context.config.id]",
31             "alConfigName": "[parameters('al').context.config.name]"
32         }
33     },
34     "hasDiskAccess": "[contains(variables('custom'), 'diskAccessId
35         ')]",
36     "storageSku": "[if(contains(variables('custom'), 'storageSku'),
37         variables('custom').storageSku, 'StandardSSD_LRS')]",
38     "trustedLaunch": "[if(contains(variables('custom'), '
39         trustedLaunch'), variables('custom').trustedLaunch, false())
40     ]"
41 }
42 ,
43 "resources": [
44     {
45         "type": "Microsoft.Compute/disks",
46         "apiVersion": "2021-08-01",
47         "name": "[variables('name')]",
48         "location": "[variables('location')]",
49         "tags": "[variables('tags')]",
50         "sku": {
51             "name": "[variables('storageSku')]"
52         }
53     },
54     {
55         "properties": {
56             "creationData": {
57                 "createOption": "Upload",
58                 "uploadSizeBytes": "[parameters('al').input.
59                     uploadSize]"
60             }
61         }
62     },
63     {
64         "incremental": "false",
```

```

59         "diskAccessId": "[if(variables('hasDiskAccess'),
60             variables('custom').diskAccessId, null())]",
61         "networkAccessPolicy": "[if(variables('hasDiskAccess'),
62             'AllowPrivate', 'AllowAll')]",
63         "publicNetworkAccess": "[if(variables('hasDiskAccess'),
64             'Disabled', 'Enabled')]",
65         "securityProfile": "[if(variables('trustedLaunch'),
66             createObject('securityType', 'TrustedLaunch'), null
67             ())]"
68     }
69 }
70 <!--NeedCopy-->

```

Imagen de arranque

La implementación de Boot Image crea una imagen de galería y una versión de imagen en la galería especificada por los datos personalizados. Muestra el ID de la versión de imagen de la galería de cómputos creada para que la utilice la plantilla **Máquina**.

Datos personalizados de Boot Image

Nombre	Tipo	Descripción	Valor predeterminado	Si son necesarias
Ubicación	cadena	La región en la que se crean los recursos.	La misma región que el grupo de recursos de destino.	no
generation	cadena	La generación de la máquina virtual utilizada en el disco.	"V2"	no

Nombre	Tipo	Descripción	Valor predeterminado	Si son necesarias
Lanzamiento confiable	booleano	true para habilitar Trusted Launch, false de lo contrario. Debe ser el mismo valor para todos los tipos de implementación.	false	no
gallery	cadena	El nombre de la galería de procesamiento en la que se va a crear la imagen. La galería debe estar en el grupo de recursos de destino.	-	sí

Plantilla de imagen de arranque

- 1.1.0.0 - Se ha añadido soporte para Trusted Launch
- 1.0.0.0 - Versión inicial

```

1 {
2
3   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/
   deploymentTemplate.json#",
4   "contentVersion": "1.1.0.0",
5   "parameters": {
6
7     "al": {
8
9       "type": "object"
10    }
11  }
12  ,
13  "variables": {
14
15    "custom": "[parameters('al').context.config.custom]",
16

```

```

17     "location": "[if(contains(variables('custom'), 'location'),
18         variables('custom').location, resourceGroup().location)]",
19     "tags": {
20         "alTaskId": "[parameters('al').context.taskId]",
21         "alUser": "[parameters('al').context.user]",
22         "alComment": "[parameters('al').context.comment]",
23         "alItemType": "[parameters('al').context.item.type]",
24         "alItemId": "[parameters('al').context.item.id]",
25         "alItemName": "[parameters('al').context.item.name]",
26         "alItemVersion": "[parameters('al').context.item.version.
27             name]",
28         "alConfigId": "[parameters('al').context.config.id]",
29         "alConfigName": "[parameters('al').context.config.name]"
30     }
31 ,
32     "name": "[concat(parameters('al').context.item.name, '.',
33         replace(parameters('al').context.config.id, '-', ''), '.',
34         parameters('al').context.item.id)]",
35     "version": "[parameters('al').context.item.version.name]",
36     "galleryName": "[variables('custom').gallery]",
37     "generation": "[if(contains(variables('custom'), 'generation'),
38         variables('custom').generation, 'V2')]",
39     "trustedLaunch": "[if(contains(variables('custom'), '
40         trustedLaunch'), variables('custom').trustedLaunch, false())
41     ]"
42 }
43 ,
44     "resources": [
45     {
46         "type": "Microsoft.Compute/galleries/images",
47         "name": "[concat(variables('galleryName'), '/', variables('
48             name'))]",
49         "apiVersion": "2021-07-01",
50         "location": "[variables('location')]",
51         "tags": "[variables('tags')]",
52         "properties": {
53             "description": "[parameters('al').context.item.
54                 description]",
55             "features": "[if(variables('trustedLaunch'),
56                 createArray(createObject('name', 'SecurityType', '
57                     value', 'TrustedLaunch')), null())]",
58             "hyperVGeneration": "[variables('generation')]",
59             "osType": "Windows",
60             "osState": "Specialized",
61             "endOfLifeDate": "2030-01-01T00:00:00Z",
62             "identifier": {
63                 "publisher": "Citrix",
64                 "offer": "[parameters('al').context.config.id]",
65                 "sku": "[parameters('al').context.item.id]"

```

```
59     }
60
61     }
62   ,
63     "resources": [
64       {
65
66         "type": "versions",
67         "apiVersion": "2021-07-01",
68         "name": "[variables('version')]",
69         "location": "[variables('location')]",
70         "dependsOn": [
71           "[resourceId('Microsoft.Compute/galleries/
72             images', variables('galleryName'), variables
73               ('name'))]"
74         ],
75         "tags": "[variables('tags')]",
76         "properties": {
77           "publishingProfile": {
78             "replicaCount": 1,
79             "targetRegions": [
80               {
81                 "name": "[variables('location')]"
82               }
83             ]
84           }
85         }
86       },
87       "storageProfile": {
88         "osDiskImage": {
89           "source": {
90             "id": "[parameters('al').input.
91               source.diskId]"
92           }
93         }
94       }
95     ]
96   }
97 }
98 ]
99
100
101
102
103
104
105 ]
106 }
107
108 ],
```

```

109     "outputs": {
110         "id": {
111             "type": "string",
112             "value": "[resourceId('Microsoft.Compute/galleries/images/
113                 versions', variables('galleryName'), variables('name'),
114                 variables('version'))]"
115         }
116     }
117 }
118 }
119 }
120 }
121 <!--NeedCopy-->

```

Máquina

La implementación de la máquina crea una máquina virtual, una NIC y un disco administrado. Esta plantilla funciona con o sin especificar la implementación de la **Imagen de arranque**.

Datos personalizados de la máquina

Nombre	Tipo	Descripción	Valor predeterminado	Si son necesarias
Ubicación	cadena	La región en la que se crean los recursos.	La misma región que el grupo de recursos de destino.	no
storageSku	cadena	El nombre del SKU del disco creado.	“Standard-SSD_LRS”	no
generation	cadena	La generación de la máquina virtual.	“V2”	no

Nombre	Tipo	Descripción	Valor predeterminado	Si son necesarias
Lanzamiento confiable	booleano	true para habilitar Trusted Launch, false de lo contrario. Debe ser el mismo valor para todos los tipos de implementación.	false	no
Arranque seguro	booleano	true para habilitar Secure Boot, false de lo contrario. Esto solo se aplica si <code>trustedLaunch</code> está establecido en true .	true	no
vTPM	booleano	true para habilitar el vTPM, false de lo contrario. Esto solo se aplica si <code>trustedLaunch</code> está establecido en true .	true	no
vmSize	cadena	El tamaño de la máquina virtual que se va a crear.	“Standard_D2s_v3”	no
licenseType	cadena	El tipo de licencia local que se aplicará a la máquina virtual.	null	no

subnetId	cadena	El ID del recurso de la subred a la que se va a conectar la NIC.	-	sí
----------	--------	--	---	----

Plantilla de máquina

- 1.1.0.0 - Se ha añadido soporte para Trusted Launch
- 1.0.0.0 - Versión inicial

```

1 {
2
3   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/
   deploymentTemplate.json#",
4   "contentVersion": "1.1.0.0",
5   "parameters": {
6
7     "al": {
8
9       "type": "object"
10    }
11  }
12 ,
13 ,
14   "variables": {
15
16     "custom": "[parameters('al').context.config.custom]",
17     "location": "[if(contains(variables('custom'), 'location'),
18     variables('custom').location, resourceGroup().location)]",
19     "name": "[concat('al-', parameters('al').context.taskId)]",
20     "vmName": "[concat(variables('name'), '-vm')]",
21     "nicName": "[concat(variables('name'), '-nic')]",
22     "diskName": "[concat(variables('name'), '-disk')]",
23     "diskId": "[resourceId('Microsoft.Compute/disks', variables('
24     diskName'))]",
25     "tags": {
26
27       "alTaskId": "[parameters('al').context.taskId]",
28       "alUser": "[parameters('al').context.user]",
29       "alComment": "[parameters('al').context.comment]",
30       "alItemType": "[parameters('al').context.item.type]",
31       "alItemId": "[parameters('al').context.item.id]",
32       "alItemName": "[parameters('al').context.item.name]",
33       "alItemVersion": "[parameters('al').context.item.version.
34       name]",
35       "alConfigId": "[parameters('al').context.config.id]",
36       "alConfigName": "[parameters('al').context.config.name]"
37     }
38   },
39   "source": "[parameters('al').input.disk.image]",

```

```
37     "isFromImage": "[not(contains(variables('source'), 'diskId'))]"
38     ,
39     "generation": "[if(contains(variables('custom'), 'generation'),
40     variables('custom').generation, 'V2')]",
41     "vmSize": "[if(contains(variables('custom'), 'vmSize'),
42     variables('custom').vmSize, 'Standard_D2s_v3')]",
43     "storageSku": "[if(contains(variables('custom'), 'storageSku'),
44     variables('custom').storageSku, 'StandardSSD_LRS')]",
45     "trustedLaunch": "[if(contains(variables('custom'), '
46     trustedLaunch'), variables('custom').trustedLaunch, false()
47     )]",
48     "secureBoot": "[if(contains(variables('custom'), 'secureBoot'),
49     variables('custom').secureBoot, variables('trustedLaunch'))
50     ]",
51     "vTpm": "[if(contains(variables('custom'), 'vTpm'), variables('
52     custom').vTpm, variables('trustedLaunch'))]",
53     "securityProfile": {
54         "securityType": "TrustedLaunch",
55         "uefiSettings": {
56             "secureBootEnabled": "[variables('secureBoot')]",
57             "vTpmEnabled": "[variables('vTpm')]"
58         }
59     }
60     }
61     ,
62     "resources": [
63         {
64             "type": "Microsoft.Network/networkInterfaces",
65             "apiVersion": "2020-11-01",
66             "name": "[variables('nicName')]",
67             "location": "[variables('location')]",
68             "tags": "[variables('tags')]",
69             "properties": {
70                 "ipConfigurations": [
71                     {
72                         "name": "ipconfig1",
73                         "properties": {
74                             "privateIPAllocationMethod": "Dynamic",
75                             "subnet": {
76                                 "id": "[variables('custom').subnetId]"
77                             }
78                         }
79                     }
80                 ]
81             }
82         }
83     ]
84     ,
85     "primary": true,
86     "privateIPAddressVersion": "IPv4"
```

```
81         }
82     }
83     },
84     ],
85     "dnsSettings": {
86         "dnsServers": []
87     },
88     ,
89     "enableAcceleratedNetworking": false,
90     "enableIPForwarding": false
91 }
92 ,
93 {
94     "condition": "[not(variables('isFromImage'))]",
95     "type": "Microsoft.Compute/disks",
96     "apiVersion": "2021-08-01",
97     "name": "[variables('diskName')]",
98     "location": "[variables('location')]",
99     "tags": "[variables('tags')]",
100     "sku": {
101         "name": "[variables('storageSku')]"
102     },
103     ,
104     "properties": {
105         "osType": "Windows",
106         "hyperVGeneration": "[variables('generation')]",
107         "creationData": {
108             "createOption": "Copy",
109             "sourceResourceId": "[variables('source').diskId]"
110         },
111         ,
112         "diskSizeGB": "[parameters('al').input.disk.size]",
113         "networkAccessPolicy": "DenyAll",
114         "publicNetworkAccess": "Disabled"
115     }
116 },
117 {
118     "type": "Microsoft.Compute/virtualMachines",
119     "apiVersion": "2021-07-01",
120     "name": "[variables('vmName')]",
121     "location": "[variables('location')]",
122     "dependsOn": [
```

```
134         "[resourceId('Microsoft.Network/networkInterfaces',
135             variables('nicName'))]",
136         "[variables('diskId')]"
137     ],
138     "tags": "[variables('tags')]",
139     "properties": {
140         "hardwareProfile": {
141             "vmSize": "[variables('vmSize')]"
142         }
143     },
144     "securityProfile": "[if(variables('trustedLaunch'),
145         variables('securityProfile'), null())]",
146     "storageProfile": {
147         "imageReference": "[if(variables('isFromImage'),
148             createObject('id', variables('source').id), null
149             ())]",
150         "osDisk": {
151             "osType": "Windows",
152             "createOption": "[if(variables('isFromImage'),
153                 'FromImage', 'Attach')]",
154             "caching": "ReadWrite",
155             "deleteOption": "Delete",
156             "diskSizeGB": "[parameters('al').input.disk.
157                 size]",
158             "managedDisk": "[if(variables('isFromImage'),
159                 createObject('storageAccountType', variables
160                 ('storageSku')), createObject('id',
161                 variables('diskId')))]"
162         }
163     },
164     "dataDisks": []
165 },
166     "networkProfile": {
167         "networkInterfaces": [
168             {
169                 "id": "[resourceId('Microsoft.Network/
170                 networkInterfaces', variables('nicName')
171                 )]"
172             }
173         ]
174     },
175     "diagnosticsProfile": {
176         "bootDiagnostics": {
```

```
176
177         "enabled": true
178     }
179
180     }
181 ,
182     "licenseType": "[if(contains(variables('custom'), '
183         licenseType'), variables('custom').licenseType, null
184         ())]",
185     "userData": "[parameters('al').input.vm.userData]"
186 }
187
188 ],
189 "outputs": {
190
191     "diskId": {
192
193         "type": "string",
194         "value": "[reference(variables('vmName')).storageProfile.
195             osDisk.managedDisk.id]"
196     }
197 ,
198     "message": {
199
200         "type": "string",
201         "value": "[format('See [link="{
202     0 }
203     /#{
204     1 }
205     /resource/{
206     2 }
207     "]{
208     2 }
209     [/{link}.', environment().portal, tenant().tenantId, resourceId('
210         Microsoft.Compute/virtualMachines', variables('vmName')))]"
211     }
212     }
213 }
214
215 <!--NeedCopy-->
```

Imagen en capas

La implementación de imágenes en capas puede crear dos tipos de recursos: una versión de imágenes de galería y/o un disco administrado. Ambos tipos de recursos se nombran con el nombre de la plantilla de imagen de App Layering que se está publicando y su número de versión construida. El número

de versión se construye con números principales y secundarios del nombre del disco de la plantilla de imagen de App Layering. Si el nombre del disco no tiene el formato de una versión numérica (`number.number`), se `1.0` aplica de forma predeterminada. El número de parche es el número de versión de la plantilla de imagen de App Layering (el número de veces que se ha publicado). A la imagen de la galería se le asigna el nombre y a la versión de la imagen de la galería se le asigna el número de versión. Al disco gestionado se le asigna el nombre adjunto al número de versión.

La imagen y la versión de la galería se crean en la galería especificada por los datos personalizados. Cuando una imagen se publica varias veces, se agrega una nueva versión a la imagen de la galería de cómputos y se conserva la versión anterior.

Datos personalizados de imágenes en capas

R = Obligatorio, O = Opcional, - = No se utiliza

Nombre	Tipo	Descripción	Valor predeterminado	Imagen de la galería	Disco administrado
Publicar como	cadena o matriz	El tipo de recurso (s) que se van a crear. Se especifica como una matriz o cadena que consta de «GalleryImage» y/o «Managed-Disk»	[“galleryImage”]	O	R
Ubicación	cadena	La región donde se crean los recursos.	La misma región que el grupo de recursos de destino	O	O
generation	cadena	La generación de la máquina virtual que admitirá la imagen.	“V2”	O	O

Nombre	Tipo	Descripción	Valor prede-terminado	Imagen de la galería	Disco administrado
Lanzamiento confiable	booleano	true para habilitar Trusted Launch, false de lo contrario. Debe ser el mismo valor para todos los tipos de implementación.	false	0	0
gallery	cadena	El nombre de la galería de procesamiento en la que se va a crear la imagen. La galería debe estar en el grupo de recursos de destino.	-	R	-
Recuento de réplicas	number	El número pre-determinado de réplicas por región de la versión de la imagen de la galería	1	0	-

Nombre	Tipo	Descripción	Valor predefinido	Imagen de la galería	Disco administrado
Regiones objetivo	matriz	Las regiones de destino de la versión de la imagen de la galería. Se especifica como una matriz de cadenas de nombres de regiones u objetos TargetRegion . La matriz debe contener la región del disco de origen (según lo especificado en los location datos personalizados).	La región especificada por los location datos personalizados	0	-
storageSku	cadena	El nombre del SKU que se va a utilizar.	“Standard-SSD_LRS”	-	0

Nombre	Tipo	Descripción	Valor prede-terminado	Imagen de la galería	Disco administrado
diskAccessId	cadena	El ID de recurso del acceso al disco que se utilizará al cargar el contenido del disco. Si se especifica, el disco se crea con el acceso a la red pública desactivado.	null	-	0

Plantilla de imagen en capas

- 1.1.0.0
 - Se agregó soporte para Trusted Launch
 - Se agregó compatibilidad con el recuento de réplicas y la región de destino para las versiones de imágenes de la galería
 - Se agregó soporte para publicar como un disco administrado
- 1.0.0.0 - Versión inicial

```
1 {
2
3   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/
4     deploymentTemplate.json#",
5   "contentVersion": "1.1.0.0",
6   "parameters": {
7     "al": {
8       "type": "object"
9     }
10  },
11  ,
12  "variables": {
13
14
15
```

```

16     "invalidChars": [ " ", "(", ")", "[", "]", "{
17     ", " }
18     ", "!", "@", "#", "$", "%", "^", "&", "*", "+", "/", "\", "'", "\"",
19     "|", "`", "~", "<", ">", ",", "?", "*" ],
20     "numericChars": [ "0", "1", "2", "3", "4", "5", "6", "7", "8",
21     "9" ],
22     "custom": "[parameters('al').context.config.custom]",
23     "location": "[if(contains(variables('custom'), 'location'),
24     variables('custom').location, resourceGroup().location)]",
25     "name": "[join(split(parameters('al').context.item.name,
26     variables('invalidChars')), '_')]",
27     "tags": {
28         "alTaskId": "[parameters('al').context.taskId]",
29         "alUser": "[parameters('al').context.user]",
30         "alComment": "[parameters('al').context.comment]",
31         "alItemType": "[parameters('al').context.item.type]",
32         "alItemId": "[parameters('al').context.item.id]",
33         "alItemName": "[parameters('al').context.item.name]",
34         "alItemVersion": "[parameters('al').context.item.version.
35         name]",
36         "alConfigId": "[parameters('al').context.config.id]",
37         "alConfigName": "[parameters('al').context.config.name]"
38     }
39     ,
40     "splitVer": "[split(parameters('al').input.diskName, '.')]",
41     "major": "[if(equals(0, length(join(split(variables('splitVer')
42     [0], variables('numericChars')), '))), variables('splitVer')
43     [0], '1')]",
44     "minor": "[if(greater(length(variables('splitVer')), 1), if(
45     equals(0, length(join(split(variables('splitVer')[1],
46     variables('numericChars')), '))), variables('splitVer')[1],
47     '0'), '0')]",
48     "version": "[format('{
49     0 }
50     .{
51     1 }
52     .{
53     2 }
54     ', variables('major'), variables('minor'), parameters('al').context.
55     item.version.number)]",
56     "galleryName": "[variables('custom').gallery]",
57     "generation": "[if(contains(variables('custom'), 'generation'),
58     variables('custom').generation, 'V2')]",
59     "trustedLaunch": "[if(contains(variables('custom'), '
60     trustedLaunch'), variables('custom').trustedLaunch, false())
61     ]",
62     "replicaCount": "[if(contains(variables('custom'), '
63     replicaCount'), variables('custom').replicaCount, 1)]",
64     "targetRegions": "[if(contains(variables('custom'), '
65     targetRegions'), variables('custom').targetRegions,
66     createArray(variables('location'))]",
67     "diskName": "[format('{

```

```

52  0 }
53  _{
54  1 }
55  -{
56  2 }
57  -{
58  3 }
59  ', variables('name'), variables('major'), variables('minor'),
    parameters('al').context.item.version.number)]",
60    "hasDiskAccess": "[contains(variables('custom'), 'diskAccessId'
    )]",
61    "storageSku": "[if(contains(variables('custom'), 'storageSku'),
    variables('custom').storageSku, 'StandardSSD_LRS')]",
62    "publishAs": "[if(contains(variables('custom'), 'publishAs'),
    variables('custom').publishAs, createArray('galleryImage'))
    ]",
63    "galleryLink": "[format('[link="{
64  0 }
65  /#@{
66  1 }
67  /resource/{
68  2 }
69  "]{
70  2 }
71  [/link].', environment().portal, tenant().tenantId, resourceId('
    Microsoft.Compute/galleries/images/versions', variables('
    galleryName'), variables('name'), variables('version')))]",
72    "diskLink": "[format('[link="{
73  0 }
74  /#@{
75  1 }
76  /resource/{
77  2 }
78  "]{
79  2 }
80  [/link].', environment().portal, tenant().tenantId, resourceId('
    Microsoft.Compute/disks', variables('diskName')))]",
81    "outputLinks": "[filter(createArray(if(contains(variables('
    publishAs'), 'galleryImage'), variables('galleryLink'), null
    ()), if(contains(variables('publishAs'), 'managedDisk'),
    variables('diskLink'), null()), lambda('link', not(equals(
    lambdaVariables('link'), null())))))]"
82  }
83  ,
84  "resources": [
85    {
86
87      "condition": "[contains(variables('publishAs'), '
    galleryImage')]",
88      "type": "Microsoft.Compute/galleries/images",
89      "name": "[format('{
90  0 }
91  /{

```

```
92 1 }
93 ', variables('galleryName'), variables('name'))]",
94     "apiVersion": "2021-07-01",
95     "location": "[variables('location')]",
96     "properties": {
97
98         "description": "[parameters('al').context.item.
99             description]",
100        "features": "[if(variables('trustedLaunch'),
101            createArray(createObject('name', 'SecurityType', '
102                value', 'TrustedLaunch')), null())]",
103        "hyperVGeneration": "[variables('generation')]",
104        "osType": "Windows",
105        "osState": "Specialized",
106        "endOfLifeDate": "2030-01-01T00:00:00Z",
107        "identifier": {
108
109            "publisher": "AppLayering",
110            "offer": "[variables('name')]",
111            "sku": "[variables('generation')]"
112        }
113    },
114    "tags": "[variables('tags')]",
115    "resources": [
116    {
117        "condition": "[contains(variables('publishAs'), '
118            galleryImage')]",
119        "type": "versions",
120        "apiVersion": "2022-03-03",
121        "name": "[variables('version')]",
122        "location": "[variables('location')]",
123        "dependsOn": [
124            "[resourceId('Microsoft.Compute/galleries/
125                images', variables('galleryName'), variables
126                ('name'))]"
127        ],
128        "tags": "[variables('tags')]",
129        "properties": {
130
131            "publishingProfile": {
132
133                "replicaCount": "[variables('replicaCount')
134                    ]",
135                "targetRegions": "[map(variables('
136                    targetRegions'), lambda('item', if(
137                        contains(lambdaVariables('item'), 'name'
138                    ), lambdaVariables('item'), createObject
139                    ('name', lambdaVariables('item')))))]"
140            }
141        }
142    },
143    ]
144 }
```

```
134         "storageProfile": {
135             "osDiskImage": {
136                 "source": {
137                     "id": "[parameters('al').input.
138                         source.diskId]"
139                 }
140             }
141         }
142     }
143 }
144 }
145 }
146 }
147 }
148 }
149 }
150 ]
151 ]
152 }
153 ,
154 {
155     "condition": "[contains(variables('publishAs'), '
156         managedDisk')]",
157     "type": "Microsoft.Compute/disks",
158     "apiVersion": "2021-08-01",
159     "name": "[variables('diskName')]",
160     "location": "[variables('location')]",
161     "tags": "[variables('tags')]",
162     "sku": {
163         "name": "[variables('storageSku')]"
164     },
165     "properties": {
166         "osType": "Windows",
167         "hyperVGeneration": "[variables('generation')]",
168         "creationData": {
169             "createOption": "Copy",
170             "sourceResourceId": "[parameters('al').input.source
171                 .diskId]"
172         }
173     },
174     "diskAccessId": "[if(variables('hasDiskAccess'),
175         variables('custom').diskAccessId, null())]",
176     "networkAccessPolicy": "[if(variables('hasDiskAccess'),
177         'AllowPrivate', 'AllowAll')]",
178     "publicNetworkAccess": "[if(variables('hasDiskAccess'),
179         'Disabled', 'Enabled')]"
180 }
```

```
181     }
182   },
183 ],
184 "outputs": {
185   "message": {
186     "type": "string",
187     "value": "[if(empty(variables('outputLinks')), null(),
188       format('See {
189     0 }
190     .', join(variables('outputLinks'), ' and ')))]"
191   }
192 }
193 }
194 }
195 }
196 }
197 }
198 }
199 <!--NeedCopy-->
```

Parámetros de plantilla

June 27, 2024

En este artículo se describen los objetos que se pasan a todas las plantillas asociadas a un conector de Azure Deployments. El objeto se pasa como parámetro `al` y se puede acceder a él mediante la función de plantilla ARM `parameters`; por ejemplo, `[parameters('al').context.user]`.

```
1 {
2   "input":
3   {
4     "type": "BootImage",
5     "source": "any"
6   }
7   ,
8   // OR
9   {
10    "type": "CacheDisk",
11    "size": "number",
12    "uploadSize": "number"
13  }
14  ,
15  // OR
16  {
17  }
18  }
19  }
```

```
21     "type": "LayeredImage",
22     "diskName": "string",
23     "source": "any"
24   }
25 ,
26 // OR
27 {
28
29   "type": "Machine",
30   "disk": {
31
32     "image": "any",
33     "size": "number",
34     "name": "string"
35   }
36 ,
37   "vm": {
38
39     "userData": "string"
40   }
41
42 }
43 ,
44 "context": {
45
46   "taskId": "number",
47   "type": "string",
48   "user": "string",
49   "comment": "string",
50   "config": {
51
52     "id": "string",
53     "name": "string",
54     "custom": "any"
55   }
56 ,
57   "item": {
58
59     "type": "string",
60     "id": "number",
61     "name": "string",
62     "description": "string",
63     "created": "string",
64     "modified": "string",
65     "version": {
66
67       "number": "number",
68       "name": "string",
69       "description": "string",
70       "created": "string"
71     }
72
73 }
```

```

74
75     }
76
77   }
78
79 <!--NeedCopy-->

```

ALParam

El conjunto de datos que se pasa a cada implementación como parámetro *al* . Se puede acceder a ella desde la plantilla ARM pasando *todo* a la función de plantilla ARM de [parámetros](#) , como `parameters('al')`.

Nombre	Descripción	Valor
input	Conjunto de datos que se aplica solo a un tipo de implementación específico. El tipo de esta propiedad depende del tipo de implementación especificado por <code>context.type</code>	BootImageInput, CacheDiskInput, LayeredImageInput, MachineInput
context	Un conjunto de datos que se aplica a todos los tipos de implementación.	Contexto de implementación

BootImageInput

Introduzca datos específicos del tipo de implementación de BootImage.

Nombre	Descripción	Valor
type	El tipo de implementación al que se aplica esta entrada.	“BootImage”

Nombre	Descripción	Valor
source	El origen de la imagen. Se trata de un objeto con una propiedad para cada salida especificada en la plantilla ARM asociada a la implementación del disco de caché .	any

“CacheDiskInput”

Introduzca datos específicos del tipo de implementación de CacheDisk.

Nombre	Descripción	Valor
type	El tipo de implementación al que se aplica esta entrada.	“CacheDisk”
size	El tamaño del disco gestionado que se va a crear, en GiB.	number (entero de 32 bits)
uploadSize	El tamaño del disco de origen que se cargará en el disco creado, en bytes.	number (entero de 64 bits)

LayeredImageInput

Introduzca los datos específicos del tipo de implementación de LayeredImage.

Nombre	Descripción	Valor
type	El tipo de implementación al que se aplica esta entrada.	“LayeredImage”
diskName	El nombre del disco tal como se especifica en la plantilla de imagen de App Layering de la imagen que se está publicando actualmente.	string

App Layering

Nombre	Descripción	Valor
source	El origen de la imagen. Se trata de un objeto con una propiedad para cada salida especificada en la plantilla ARM asociada a la implementación de la Máquina .	any

MachineInput

Introduzca datos específicos del tipo de implementación de la máquina.

Nombre	Descripción	Valor
type	El tipo de implementación al que se aplica esta entrada.	“Machine”
disk	Datos de entrada que se aplican al disco del sistema operativo de la máquina.	DiskInput
vm	Datos de entrada que se aplican a la propia máquina virtual.	VmInput

DiskInput

Datos de entrada que se aplican al disco del sistema operativo de una máquina.

Nombre	Descripción	Valor
image	El origen del disco. Se trata de un objeto con una propiedad para cada salida especificada en la plantilla ARM asociada a la implementación de la imagen de arranque , si la implementación de la imagen de arranque se especifica en la configuración del conector. Si no se especifica la implementación de la imagen de arranque , se utiliza la salida de la plantilla ARM asociada a la implementación del disco de caché .	any
size	Tamaño del disco que se va a crear, en GiB.	number (entero de 64 bits)
name	El nombre del disco tal como se especifica en la plantilla de imagen de App Layering de la imagen que se está publicando actualmente. Si no se trata de una operación de publicación de imágenes, entonces no está definida.	string

VmInput

Datos de entrada que se aplican a una máquina virtual.

Nombre	Descripción	Valor
userData	El valor que se debe aplicar a la propiedad <code>userData</code> de <code>VirtualMachineProperties</code> del valor <code>virtualMachine</code> especificado en la plantilla ARM asociada a la implementación.	string

DeploymentContext

Proporciona el contexto de la operación de implementación actual.

Nombre	Descripción	Valor
taskId	El ID de la tarea de ELM que provocó la implementación.	number (entero de 64 bits)
type	El tipo de implementación actual.	'CacheDisk', 'BootImage', 'Machine', 'LayeredImage'
user	El nombre de usuario que inició la tarea de ELM que provocó esta implementación.	string
comment	El comentario que el usuario introdujo al iniciar la tarea de ELM que provocó esta implementación.	string
config	La configuración del conector de plataforma que está asociada a esta implementación.	Config
item	La entidad de App Layering asociada a la tarea de ELM que provocó esta implementación. Se referirá a una capa, una plantilla de imagen en capas o una imagen de arranque.	Elemento

Config

Contiene las propiedades de la configuración del conector de plataforma asociada a la operación actual.

Nombre	Descripción	Valor
id	El ID de la configuración del conector de la plataforma. Se trata de un guid con el formato <code>XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</code> .	string
name	El nombre de la configuración del conector de plataforma.	string
custom	Los datos personalizados especificados en la configuración del conector de plataforma. El tipo y las propiedades de este objeto dependen del JSON especificado por el usuario para el tipo de implementación actual.	any

Elemento

La entidad de App Layering asociada a una tarea de ELM que provocó una implementación.

Puede ser una capa, una plantilla de imagen en capas o una imagen de arranque.

Nombre	Descripción	Valor
type	El tipo de elemento de la entidad de App Layering.	'Image', 'AppLayer', 'OsLayer', 'PlatformLayer', 'Connector-CachedCeBootApplication'
id	El identificador del artículo.	number (entero de 64 bits)
name	El nombre del artículo.	string
description	La descripción del artículo.	string

App Layering

Nombre	Descripción	Valor
created	La fecha y la hora en que se creó originalmente el elemento.	string (fecha y hora ISO 8601)
modified	La fecha y la hora en que se modificó el artículo por última vez.	string (fecha y hora ISO 8601)
version	Información sobre esta versión específica del artículo.	Versión

Versión

La versión de una entidad de App Layering asociada a una tarea de ELM que provocó una implementación. Puede ser una versión de capa, una versión de plantilla de imagen en capas o una versión de imagen de arranque.

Nombre	Descripción	Valor
number	Un entero que representa la versión. En el caso de las capas, este es el número de intentos de empaquetado. En el caso de las plantillas de imágenes en capas, este es el número de publicaciones exitosas de la plantilla. Para las imágenes de arranque, esta es la marca de tiempo del archivo de imagen.	number (entero de 32 bits)
name	El nombre de la versión. Para las capas, este es el nombre de la versión especificado por el usuario. Para las plantillas de imágenes en capas, esto es <i>Publish {Number}_</i> . Para las imágenes de arranque, esta es la versión (x.y.z) de App Layering que crea la implementación.	string

Nombre	Descripción	Valor
description	Descripción de la versión. Para las capas, esta es la descripción de la versión especificada por el usuario. En el caso de las plantillas de imágenes en capas, se trata de una cadena vacía. Para las imágenes de arranque, se trata de una descripción genérica que incluye el número de versión del dispositivo.	string
created	La fecha y la hora en que se creó la versión. En el caso de las capas, es cuando se creó la versión. En el caso de las plantillas de imágenes en capas, esta es la última vez que se editó la plantilla. Para las imágenes de arranque, esta es la marca de tiempo del archivo de imagen.	string (fecha y hora ISO 8601)

XenServer

May 9, 2024

XenServer es una plataforma de hipervisor altamente optimizada para Citrix Virtual Apps and Desktops, que permite la entrega de aplicaciones y escritorios virtuales de Windows y Linux a cualquier dispositivo y a cientos de empleados en solo unos minutos.

Antes de comenzar

Puede usar el entorno de XenServer para crear capas y publicar imágenes en capas. Cada configuración de Connector accede a una ubicación de almacenamiento específica en el entorno de XenServer. Es posible que necesite más de una configuración de XenServer Connector para acceder

a la ubicación correcta para cada propósito. Además, puede publicar cada imagen en capas en una ubicación conveniente para el sistema que aprovisiona con la imagen publicada. Para obtener más información sobre los conectores y las configuraciones de conectores, consulte [Configuraciones de conectores](#).

Con la arquitectura XenServer, puede interactuar con servidores individuales o con un clúster de servidores en lugar de con un servidor de administración central. Puede administrar XenServer mediante software de administración o acceso por línea de comandos, como XenCenter. Puede instalar XenCenter en el escritorio y conectarse de forma individual a cada host o a un clúster de hosts.

Si esta es la primera vez que usa App Layering

Si quiere crear capas de aplicaciones mediante una máquina virtual de XenServer, necesita un conector de XenServer en App Layering. Al publicar imágenes en capas en XenServer, también necesita una configuración de conector para cada una de las ubicaciones de publicación.

Al crear una capa y publicar una imagen en capas, se le pide que seleccione una configuración de conector. Si aún no tiene la configuración de conectores correcta para la tarea, puede crear una haciendo clic en **Agregar configuración de conectores** en la página **Conectores**.

Información necesaria para los parámetros de configuración del conector de XenServer

La configuración de un conector para XenServer le permite buscar el **servidor XenCenter**, el **almacén de datos** y el **host** para usarlos en una nueva configuración.

Importante

Los campos distinguen entre mayúsculas y minúsculas. Todos los valores que introduzca manualmente deben coincidir con las mayúsculas y minúsculas del objeto en XenServer; de lo contrario, se producirá un error en la validación.

- **Nombre de configuración de XenServer:** un nombre útil para ayudar a identificar y realizar un seguimiento de esta configuración de conector.
- **Dirección de XenServer:** nombre del host de XenServer con el que se integra el dispositivo.
- **Nombre de usuario y contraseña:** las credenciales de la cuenta que usa el dispositivo para conectarse a XenServer.
- **Utilice comunicaciones seguras:** cifrado SSL para el tráfico de conexión de API entre App Layering Connector y XenServer. Este campo está seleccionado de forma predeterminada.
- **Plantilla de máquina virtual: la plantilla** de máquina virtual para la clonación. La lista de opciones contiene solo plantillas de máquinas virtuales personalizadas, en lugar de máquinas virtuales reales o cualquiera de las plantillas integradas. La plantilla seleccionada no debe tener ningún disco conectado y debe tener al menos una tarjeta de red conectada. Si no lo hace, verá un error al intentar validar o guardar la configuración.

- **Repositorio de almacenamiento:** el repositorio de almacenamiento del disco que se carga. La lista se filtra para mostrar solo los repositorios que pueden contener discos duros virtuales (los repositorios ISO se filtran).
- **Tamaño de la caché de disco de la capa en GB (opcional):** especifica el tamaño de la caché permitido para la capa. De forma predeterminada, el tamaño de caché permitido es de 250 GB.
- **Utilice HTTPS para las transferencias de archivos:** cifra las transferencias de archivos de imágenes. HTTPS está seleccionado de forma predeterminada para cargas y descargas más seguras, pero se puede borrar para aumentar el rendimiento. Esto no se aplica cuando se habilita la composición de descargas.
- **Composición de descarga (recomendado): permite que** el proceso de empaquetado de capas o publicación de imágenes se ejecute en el servidor de hipervisor especificado. Esta función aumenta el rendimiento y permite utilizar el formato de disco VMDK y máquinas virtuales BIOS o UEFI. Con UEFI, también puedes usar Secure Boot si está habilitado en el hipervisor.
- **Repositorio de almacenamiento ISO:** repositorio para los discos que carga Offload Compositing. La lista se filtra para mostrar solo los repositorios ISO. Se admiten SMB y NFS.
- **Ruta de compartición ISO:** se rellena automáticamente para el repositorio de almacenamiento ISO seleccionado según la ruta de compartición ISO configurada. Solo para visualización.
- **Nombre de usuario del recurso compartido ISO:** nombre de usuario del recurso compartido ISO seleccionado. Solo válido para SMB ISO Share. NFS ISO Share no admite un nombre de usuario ni una contraseña.
- **Contraseña de compartición ISO:** Contraseña para el recurso compartido ISO seleccionado. Solo válido para SMB ISO Share. NFS ISO Share no admite un nombre de usuario ni una contraseña.

Cuando se selecciona Descarga de composición:

- Si proporciona una plantilla configurada para BIOS o UEFI, la máquina virtual resultante será del tipo que haya elegido.
- Si proporciona una plantilla con UEFI-Secure Boot habilitado y seleccionado, la máquina virtual resultante es UEFI-Secure Boot.

Si la opción Descargar composición no está seleccionada:

- Si proporciona una plantilla configurada para BIOS, la máquina virtual resultante es BIOS.
- Si proporciona una plantilla configurada para UEFI y cuando intenta guardar la configuración del conector, aparece un error.

Carpeta de máquinas virtuales

Las máquinas virtuales creadas por el conector de XenServer, ya sean máquinas de empaquetado o imágenes en capas, pueden usar carpetas o etiquetas para organizar las máquinas virtuales. XenServer le permite organizar las máquinas virtuales por carpeta o por etiqueta. Estas herramientas organizativas son opcionales al crear y administrar máquinas virtuales a través de XenCenter u otras

herramientas. Aunque las configuraciones del conector de XenServer no permiten especificar carpetas o etiquetas, las máquinas virtuales creadas por el conector de XenServer, tanto las máquinas de empaquetado como las imágenes en capas publicadas, pueden usar ambas herramientas organizativas.

Etiquetas de almacenamiento en caché

Si la plantilla especificada en la configuración del conector de XenServer tiene etiquetas, esas etiquetas se transfieren a cualquier máquina virtual clonada a partir de esa plantilla. Todas las máquinas virtuales de empaquetado o las imágenes en capas publicadas se etiquetan con las mismas etiquetas que tiene la plantilla. Además, el conector de XenServer agrega tres etiquetas.

- **App Layering:** Todas las máquinas virtuales creadas por el conector de XenServer se pueden encontrar en esta etiqueta, independientemente de su propósito o imagen.
- **Etiqueta de propósito:** Todas las máquinas de empaquetado se etiquetan con **App Layering Packaging Machine**, mientras que todas las máquinas virtuales de imágenes en capas publicadas se etiquetan con **imágenes publicadas de App Layering**.
- **Nombre de imagen o capa:** Todas las máquinas de empaquetado se etiquetan con el nombre de la capa para la que se generan, mientras que todas las imágenes en capas publicadas se etiquetan con el nombre de la imagen de la plantilla.

Si usa XenCenter, puede ver las máquinas virtuales por etiqueta; para ello, seleccione Vistas de organización y, a continuación, seleccione Por etiqueta.

Carpeta

De forma predeterminada, las máquinas virtuales creadas por el conector de XenServer no se colocan en una carpeta. Sin embargo, si la plantilla especificada en la configuración del conector de XenServer reside en una carpeta, cualquier máquina virtual que el conector cree a partir de esa plantilla también reside en la misma carpeta. Todas las máquinas virtuales de empaquetado y las imágenes en capas publicadas se colocan en la misma carpeta. No hay subcarpetas independientes para empaquetar máquinas virtuales o imágenes en capas publicadas.

Conectividad de red de máquinas

La configuración de red virtual de la plantilla de origen especificada en la configuración del conector de XenServer se transfiere al crear cualquier máquina virtual a través del conector de XenServer. No hay ninguna opción en la interfaz de usuario de configuración del conector para anular la configuración de red.

Clústeres de XenServer

El conector de XenServer aún no funciona correctamente con los clústeres de XenServer. Si el host especificado en la configuración forma parte de un clúster, debe ser el host maestro del clúster para que el conector funcione. Sin embargo, esto significa que cada vez que el host maestro de XenServer deja de funcionar y se elige un nuevo maestro, se debe actualizar la configuración de XenServer.

Crear una configuración de conector

Para introducir los valores:

- Introduzca los tres primeros campos Connector manualmente. Tras validar las credenciales de esos campos, puede seleccionar valores para los campos restantes en los menús desplegables.
- Para introducir valores manualmente, haga clic para poner el cursor en el campo y escriba el valor, asegurándose de que las mayúsculas y minúsculas coinciden con el valor en XenServer.
- Para seleccionar un valor de una lista desplegable, haga lo siguiente:
 - Haga clic una vez para colocar el cursor en el campo.
 - Haga clic una segunda vez para mostrar la lista de valores posibles.

Para agregar una configuración de conector

1. Haga clic en la página **Conectores**.
2. Haga clic en **Agregar configuración de conector**. Se abre un cuadro de diálogo.
3. Seleccione el **tipo de conector** para la plataforma y la ubicación en la que va a crear la capa o publicar la imagen.
4. Haga clic en **Nuevo** para abrir la página de configuración del conector.
5. Escriba el **nombre** de configuración, la dirección de XenServer, el nombre de usuario, la contraseña y la configuración de la casilla **Usar comunicaciones seguras**. Para obtener más información, consulta las definiciones de campo anteriores.
6. Haga clic en **CONECTAR** debajo de los campos de configuración de XenServer. A continuación, se habilitan los campos de **configuración de clonación de máquinas virtuales** si el nombre de usuario y la contraseña son correctos.

Nota:

Si hay un error en el certificado, aparece el siguiente mensaje de error:

```
One or more problems with the service certificate were found
. You can enable them to be ignored, or you must update the
certificate on the server.
```

Puede hacer clic en **Omitir errores de certificado y continuar**.

7. Seleccione la **plantilla de máquina virtual** requerida.
8. Seleccione el **repositorio de almacenamiento**.
9. Asegúrese de que el **tamaño de la caché de paquetes en GB** esté establecido en el valor deseado (o utilice el valor predeterminado). Si se establece el valor en 0, no se almacena en caché.

10. Seleccione la configuración de **Usar HTTPS para transferencias de archivos**.
11. Seleccione la configuración para **Usar composición de descarga**.
12. Si se selecciona **Usar composición de descarga, seleccione Repositorio** de almacenamiento **ISO**. La **ruta de compartición ISO** se rellena automáticamente.
13. Si se selecciona un recurso compartido **ISO de SMB**, introduzca el nombre de usuario y la contraseña del recurso **ISO de SMB**.
14. Haz clic en **CONFIRMAR Y COMPLETAR**. Se muestra un resumen de la configuración.
15. Haga clic en **Guardar**. Si no se muestra ningún error, la nueva configuración del conector se guarda y se muestra en la página **Conector**.

Citrix Provisioning (XenServer, VMware, Hyper-V, Nutanix)

May 9, 2024

La configuración del conector de Citrix Provisioning requiere una cuenta que el dispositivo de App Layering pueda utilizar para acceder a la máquina virtual en la que está creando una capa o publicando imágenes en capas.

Cuando se usa vSphere como hipervisor para Citrix Provisioning, se recomienda usar la misma plantilla de máquina virtual de vSphere, en la configuración del conector de vSphere, para crear capas como lo hace para crear los dispositivos de destino en Citrix Provisioning. Esta práctica garantiza que la imagen publicada y los dispositivos de destino tengan las mismas especificaciones de máquina virtual de referencia.

Requisitos

Si planea publicar imágenes en capas en su entorno de Citrix Provisioning, agregue una configuración de conector de Citrix Provisioning para esa ubicación de Citrix Provisioning.

Requisitos de Citrix Provisioning

- Las cuentas de dominio tienen permiso para acceder al almacén de Citrix Provisioning y la cuenta del sistema local no. Si el servidor de Citrix Provisioning está configurado para utilizar la cuenta de sistema local, que es la configuración predeterminada, puede cambiar la cuenta ejecutando el asistente de configuración de Citrix Provisioning. El asistente le ofrece la opción de ejecutarlo como **sistema local** o usar una **cuenta de dominio**. Elige una **cuenta de dominio**.

- La cuenta de usuario de dominio en la configuración del conector debe estar en el grupo Administradores local del servidor Citrix Provisioning.
- Información de cuenta y servidor de Citrix Provisioning: para que App Layering acceda a la ubicación del entorno de Citrix Provisioning en la que quiere publicar una imagen en capas, debe proporcionar las credenciales y la ubicación en una configuración del conector de Citrix Provisioning.
- El agente de App Layering debe estar instalado en cada uno de los servidores de Citrix Provisioning. Para obtener más información, consulte las instrucciones de instalación del agente.

Configuración del conector de Citrix Provisioning

La información que necesita para la configuración del conector de Citrix Provisioning incluye.

- **Nombre de configuración:** Nombre útil para identificar y realizar un seguimiento de la configuración de este conector.

Configuración del servidor Citrix Provisioning

- **Consola:** El *nombre* del servidor de Citrix Provisioning en el que se implementa el agente de App Layering. Este es el servidor en el que se publica el disco Personal vDisk.

Nota:

El nombre de host es necesario, en lugar del FQDN, para que el servidor Citrix Provisioning pueda acceder al dispositivo de App Layering si se encuentra en un dominio diferente.

- **Usuario de dominio:** Nombre de usuario de una cuenta de dominio que tiene permiso para administrar Citrix Provisioning. El agente utiliza esta cuenta para ejecutar comandos de PowerShell de Provisioning Services. Esta cuenta debe tener acceso de **lectura y escritura** al almacén de Citrix Provisioning para escribir el disco Personal vDisk publicado.
- **Contraseña:** La contraseña de la cuenta de usuario del dominio.

Configuración de discos virtuales

- **Nombre del sitio:** Nombre del sitio al que pertenecerá este disco Personal vDisk.
- **Nombre del almacén:** Nombre del almacén al que pertenece este disco Personal vDisk.
- **Caché de escritura:** Cuando se crea un disco nuevo, este valor establece el tipo de **caché de escritura** del nuevo disco. Los valores posibles incluyen:
 - Caché en el servidor
 - Caché en el servidor, persistente

- Caché en la memoria RAM del dispositivo
- Caché en la memoria RAM del dispositivo con desbordamiento en el disco duro
- Caché en el disco duro del dispositivo

Importante:

Al elegir una opción de **escritura en memoria caché**, consulte [Selección del destino de la memoria caché de escritura para las imágenes de disco Personal vDisk estándar para](#) asegurarse de que los servidores de Citrix Provisioning y los dispositivos de destino que usan este disco Personal vDisk estén configurados correctamente para el tipo que seleccione.

- **Modo de licencia:** Establece el modo de licencia de Windows en:
 - KMS: Servicio de gestión de claves
 - MAK: Varias claves de activación
 - Ninguno
- **Habilitar la administración de contraseñas de cuentas de máquinas de Active Directory:** Habilita la administración de contraseñas de Active. El valor predeterminado es **Habilitado**.
- **Habilitar equilibrio de carga:** Habilita el equilibrio de carga. para la transmisión por secuencias del disco Personal vDisk.
- **Habilitar la administración de impresoras:** Cuando está habilitada, las impresoras no válidas se eliminan del dispositivo.

Configuración de composición Configuración del conector de descarga: Una configuración de conector de hipervisor con la **composición de descarga** habilitada. Esta configuración de conector compone capas en nombre del conector de Citrix Provisioning. La configuración de la máquina virtual que utiliza el motor de composición de descarga proviene de esta configuración de conector. Por ejemplo, si la configuración del conector de descarga está configurada para crear máquinas UEFI, el disco virtual resultante está en formato UEFI.

Formato de disco: El formato de disco del disco virtual de Citrix Provisioning en el servidor de Citrix Provisioning. El formato especificado aquí anula el formato en la configuración del conector de descarga asociada.

Ruta de recurso compartido de archivos: La ruta UNC correspondiente al almacén de Citrix Provisioning seleccionado en la configuración del disco virtual. Los requisitos incluyen:

- Si el almacén de Citrix Provisioning no apunta a un recurso compartido de archivos UNC, configure la ruta local como un recurso compartido SMB.
- La ruta del recurso compartido de archivos es accesible para el motor de composición y para el almacén de Citrix Provisioning seleccionado.

Si cambia la selección de almacén cuando se selecciona Descargar composición, el conector intentará resolver la ruta del recurso compartido de archivos. Si la ruta del recurso compartido de archivos no se puede resolver automáticamente, permanece en blanco.

Configuración de scripts (opcional, función avanzada)

Al crear una configuración de conector, puede configurar un script opcional de PowerShell en cualquier máquina Windows que ejecute un agente de App Layering, el mismo agente utilizado en el servidor de Citrix Provisioning. Almacene estos scripts en el equipo donde está instalado el agente de App Layering. Ejecute los scripts solo después de una implementación correcta de una imagen en capas. Algunas variables preestablecidas están disponibles para permitir que los scripts sean reutilizables con diferentes imágenes de plantilla y configuraciones de conectores diferentes. Estas variables también contienen información necesaria para identificar la máquina virtual creada como parte de la imagen en capas publicada en Citrix Provisioning.

La ejecución de los scripts no afecta al resultado del trabajo de publicación y el progreso de los comandos ejecutados en el script no está visible. Los registros del conector de Citrix Provisioning contienen la salida del script que se ejecutó.

Configurar un script

Recuerde que este procedimiento es opcional. Si quiere que se ejecute un script cada vez que se publique una imagen en capas, siga estos pasos mediante los valores descritos en las secciones siguientes.

1. Complete y guarde la configuración del conector.

Nota:

Antes de seleccionar la página Configuración de script, debe guardar (o descartar) cualquier modificación en los parámetros de configuración del conector.

2. Si el menú Navegación de la izquierda no está abierto, selecciónelo y haga clic en **Configuración de scripts** para abrir la página Ruta del script.
3. Complete los campos obligatorios y haga clic en **Guardar**. A continuación se describen los campos.

Campos de configuración de scripts

- **Habilitar scripts:** Seleccione esta casilla de verificación para habilitar los campos restantes. Esto le permite introducir un script que se ejecuta cada vez que se publica una imagen en capas.

- **Agente de scripts:** La máquina agente en la que se encuentran y se ejecutan los scripts.
- **Nombre de usuario (opcional):** el nombre de usuario que se va a *suplantar* al ejecutar el script. Este nombre se puede utilizar para garantizar que el script se ejecuta en el contexto de un usuario que tiene los derechos/permisos necesarios para realizar las operaciones en el script.
- **Contraseña (opcional):** la contraseña del nombre de usuario especificado.
- **Ruta de script: ruta** de acceso completa y nombre de archivo en la máquina agente en la que reside el archivo de script.

Otros valores de configuración de scripts

Variables de PowerShell Utilice cualquiera de estas variables en el script de PowerShell:

Valor	Se aplica a tipos de conectores	Valor determinado por el código	Descripción
connectorCfgName	Todo	Código común	Nombre de la configuración del conector con la que está asociada la configuración del script.
imageName	Todo	Código común	Nombre de la plantilla de imagen en capas que se utiliza para crear/publicar la imagen en capas.
osType	Todo	Código común	Tipo de sistema operativo de la imagen en capas publicada. Puede ser uno de los siguientes valores: Windows7; Windows764; Windows200864; Windows201264; Windows10; Windows1064
diskLocatorId	Todo	Provisioning Services	El ID interno del disco Personal vDisk.

Suplantación de usuario El Agente de App Layering, que se ejecuta como un servicio en un equipo Windows, se ejecuta en la cuenta del sistema local o en la cuenta de red. Cualquiera de estas cuentas puede tener algunos privilegios especiales, pero a menudo están restringidos cuando se ejecutan comandos específicos o se ven archivos en el sistema de archivos. Por lo tanto, App Layering le da la opción de agregar un usuario de dominio y una contraseña que se pueden usar para “suplantar” a un usuario. Esto significa que el script se puede ejecutar como si ese usuario hubiera iniciado sesión en el sistema para que cualquier comando o dato sea accesible sujeto a esos derechos y permisos de usuario. Si no se introduce un nombre de usuario o una contraseña, el script se ejecuta mediante la cuenta en la que el servicio está configurado para ejecutarse.

Directiva de ejecución de scripts Los requisitos de la directiva de ejecución de scripts dependen de usted. Si tiene intención de ejecutar scripts sin firmar, debe configurar la directiva de ejecución en una de las directivas más indulgentes. Sin embargo, si firma sus propios scripts, puede optar por utilizar una directiva de ejecución más restrictiva.

Cloud de Google

January 9, 2022

Una configuración de conector contiene las credenciales que utiliza el dispositivo para acceder a un proyecto específico en Google Cloud. Necesitas una configuración de conector para cada proyecto de Google Cloud al que quieras acceder con el dispositivo.

La creación de capas en Google Cloud requiere una configuración del conector de Google Cloud. En este artículo se describen los valores necesarios para el conector. Consulte [Configuraciones de conectores](#) para obtener más información sobre las configuraciones y cómo crearlas.

Antes de crear una configuración de conector de Google Cloud

En esta sección se explica:

- La información de la cuenta de Google Cloud necesaria para crear esta configuración de conector.
- El almacenamiento de Google Cloud que necesitas para App Layering.

Clave de cuenta de servicio y cuenta de servicio de Google Cloud requeridas

La configuración del conector de Google Cloud requiere la siguiente información.

- **Proyecto** : ID del proyecto de un proyecto de Google Cloud.
- **Archivo de clave de cuenta de servicio** : para realizar llamadas a la API como cuenta de servicio en nombre de la configuración del conector.
- **Almacenamiento**: ubicación de almacenamiento en Google Cloud para almacenar discos virtuales cargados por el conector.
- **Plantilla de instancias**: **plantilla** de máquina virtual de Google Cloud con la configuración deseada para crear una máquina virtual.
- **Tipo de disco**: tipo de [Almacenamiento de Google Cloud](#).
- **Zona**: Google Cloud Zone en la que planeas crear capas o publicar imágenes mediante la configuración del conector.

Depósito de almacenamiento de Google Cloud obligatorio

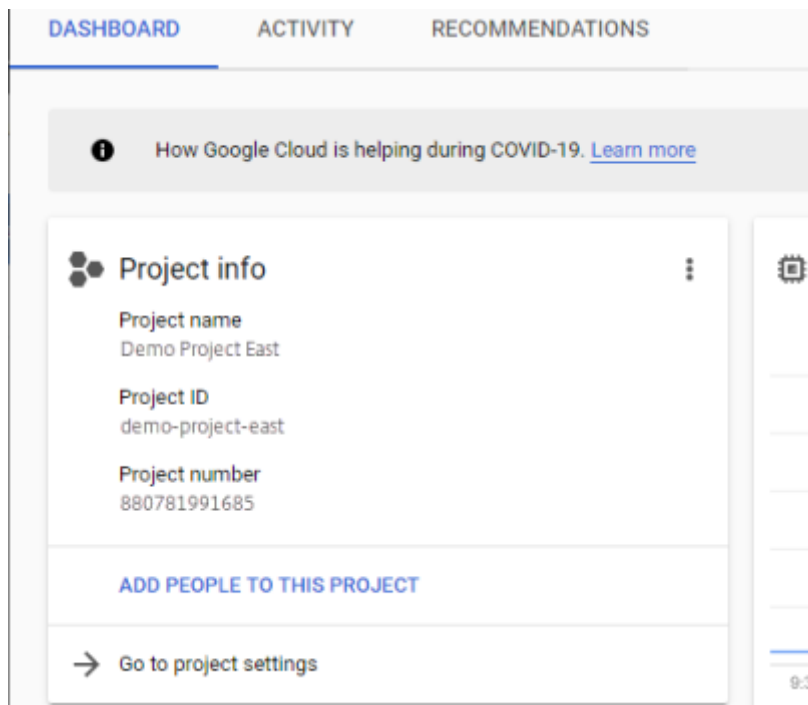
Cualquier cuenta que utilices para App Layering debe cumplir los siguientes requisitos:

- Debe estar separado del cubo de almacenamiento utilizado para el dispositivo.
- Debe encontrarse en la ubicación de Google Cloud en la que planea implementar máquinas virtuales.

Crear una cuenta de servicio de Google y un archivo de clave de cuenta de servicio

Utilice los siguientes procedimientos para cada proyecto de Google Cloud que desee conectar con el dispositivo App Layering.

1. Inicia sesión en **console.cloud.google.com**.
2. Seleccione el proyecto y haga clic en **Ir a la configuración del proyecto**.



3. En el panel izquierdo, **haz clic en Cuentas de servicio**.
4. En la parte superior de la página, haz clic en **+ CREAR CUENTA DE SERVICIO**.
5. Añade los detalles de tu cuenta de servicio
 - Nombre de esta cuenta de servicio: Nombre descriptivo. Por ejemplo, TestEast1
 - ID de cuenta de servicio: rellena lo que has puesto en el campo nombre, usa ese valor.
6. Haz clic en el botón **Crear**.

Agregue las funciones de su cuenta de servicio

En el cuadro **Seleccionar rol**, seleccione los roles necesarios:

- Administrador de almacenamiento
 - Administrador de procesos
 - Usuario de cuenta de servicio
1. Haga clic en el botón **Continuar**.
 2. Haz clic en el botón **Listo**. El acceso de los usuarios al rol no es necesario.

Crear un archivo de clave de cuenta de servicio

1. En el proyecto, selecciona la pestaña **Cuenta de servicio** situada a la izquierda.

2. Haz clic en los tres puntos verticales a la derecha de la cuenta de servicio para la que quieres crear el archivo clave.
3. Selecciona **Crear clave**.
4. En la ventana emergente, seleccione el botón de radio JSON y haga clic en el botón **CREAR**.
5. Cuando se le pida que guarde la clave en un archivo, introduzca el nombre de su elección o mantenga el nombre predeterminado. Vuelves a la pantalla Cuentas de servicio.
6. Haz clic en tu cuenta de servicio para comprobar que la clave está ahí.

Editar roles de cuenta de servicio

Para editar los roles:

1. Navega hasta la pantalla de la interfaz de usuario del proyecto tal como lo hacías al crear la cuenta de servicio.
2. En el menú de hamburguesas de la parte superior izquierda, expande **IAM y ADMIN** y selecciona **Administrar recursos**.
3. Seleccione su proyecto y, a la derecha, escriba la **cuenta de servicio** que desea editar en el árbol de filtros. Se muestra el nombre de la cuenta de servicio.
4. Edite cada uno de los roles para incluirlos o quitarlos de los roles y guardar los resultados.

Nota:

Si elimina todo el privilegio de la cuenta de servicio, ya no se mostrará en la página de IAM (porque la página de IAM solo muestra las cuentas con al menos un rol adjunto). Pero aparecerá en la pantalla Cuenta de servicio. Tendría que ir a la página de IAM para volver a agregar privilegios.

5. Haz clic en el botón **AÑADIR**.
6. En el panel **Agregar miembros, roles al proyecto «actual»**, en el campo **Nuevos miembros**, escriba el nombre del miembro al que desea otorgar privilegios.
7. Seleccione los roles que desea asignar al miembro y haga clic en el botón **GUARDAR**.

Machine Creation for Azure

June 17, 2022

Una configuración de conector contiene las credenciales y la información de ubicación que el dispositivo necesita para tener acceso a una ubicación específica en Machine Creation for Azure. Por ejemplo, su organización puede tener una cuenta de Machine Creation for Azure y varias ubicaciones de almacenamiento, y necesita una configuración de conector para que el dispositivo pueda acceder a cada ubicación de almacenamiento.

Este artículo describe las definiciones incluidas en la configuración del conector de Machine Creation for Azure. Para obtener más información sobre las configuraciones de los conectores y cómo agregarlas, consulte [Conectar](#).

Nota:

Este conector se puede usar para cualquier plantilla que desee usar en un catálogo no persistente. Por ejemplo, si implementa una plantilla en Azure y quiere usarla para crear un disco Personal vDisk de Citrix Provisioning para máquinas no persistentes, debe usar el conector MCS para publicar la plantilla.

Cuándo agregar una configuración de conector para Azure

Cuando cree las primeras capas y, posteriormente, cuando publique imágenes en capas por primera vez, agregará una configuración de conector para cada tarea, como se describe a continuación.

Información necesaria de Azure para Machine Creation for Azure

Es posible que su organización tenga varias suscripciones a Azure. Para que App Layering Service acceda a sus suscripciones de Azure, ya sea para importar una imagen del sistema operativo o publicar una imagen en capas, debe usar el procedimiento siguiente para cada suscripción de Azure a la que quiera conectarse a través de App Layering Service.

- **Nombre:** Nombre que se introduce para una nueva configuración de conector.
- **ID de suscripción:** Para implementar máquinas virtuales de Azure, su organización debe tener un ID de suscripción.
- **ID de arrendatario:** Instancia de Azure Active Directory, este GUID identifica la instancia dedicada de Azure Active Directory (AD) de su organización.
- **ID de cliente:** Identificador del registro de aplicaciones, que su organización ha creado para App Layering.
- **Secreto de cliente:** La contraseña del ID de cliente que está utilizando. Si ha olvidado el secreto del cliente, puede crear uno nuevo. > **Nota:**

Cada vez que utilice una nueva suscripción y un ID de arrendatario, debe introducir un nuevo secreto de cliente. Esto se debe a que los secretos del cliente están asociados lógicamente con los arrendatarios de Azure.

- **Nombre de la cuenta de almacenamiento:** La cuenta de almacenamiento de Azure que quiere usar para almacenar discos de máquinas virtuales de Azure. Este nombre debe cumplir con las restricciones de nombres de cuentas de almacenamiento de Azure. Por ejemplo, el nombre de la cuenta de almacenamiento no puede contener caracteres en mayúsculas.

Debe crear una cuenta de almacenamiento a través del portal o utilizar una cuenta de almacenamiento existente que se ajuste a los siguientes criterios. La cuenta:

- No puede ser una cuenta de almacenamiento clásica.
- Ser una cuenta de almacenamiento independiente de la que se utiliza para el dispositivo. Esta nueva cuenta de almacenamiento se utiliza durante la creación de capas y la publicación de imágenes en capas.
- Debe estar en la ubicación de Azure donde va a implementar máquinas virtuales.
- Debe ser uno de los siguientes tipos:
 - Almacenamiento de información con redundancia local estándar (LRS)
 - Almacenamiento de información georredundante estándar (GRS)
 - Almacenamiento de información georredundante de acceso de lectura estándar (RAGRS)
- Se puede ubicar en cualquier grupo de recursos, siempre que la ubicación del grupo de recursos sea la misma que la ubicación de la cuenta.

Machine Creation for Azure Government

November 5, 2020

Una configuración de conector contiene la información que el dispositivo necesita para tener acceso a una ubicación específica para la creación de equipos en Azure Government. Si su organización tiene más de una ubicación de almacenamiento, necesita una configuración de conector para cada ubicación.

Este artículo describe las definiciones incluidas en la configuración del conector de Machine Creation for Azure Government. Para obtener más información acerca de las configuraciones de conectores y cómo agregarlas, consulte [Conectar](#).

Cuándo agregar una configuración de conector para Azure Government

Cuando cree las primeras capas y, posteriormente, cuando publique imágenes en capas por primera vez, agregará una configuración de conector para cada tarea, como se describe a continuación.

Información de Azure Government

Es posible que su organización tenga varias suscripciones a Azure Government. Para que el servicio de App Layering tenga acceso a sus suscripciones, ya sea para importar una imagen del sistema operativo o para publicar una imagen en capas, debe utilizar el procedimiento siguiente para cada suscripción de Azure Government a la que quiera conectarse a través del servicio App Layering.

- **Nombre:** Nombre que introduce para una nueva configuración de conector.
- **ID de suscripción:** Para implementar máquinas virtuales de Azure Government, su organización debe tener un ID de suscripción.
- **ID de arrendatario:** Una instancia de Azure Government Active Directory, este GUID identifica la instancia dedicada de Azure Government Active Directory (AD) de su organización.
- **ID de cliente:** Un identificador para el registro de aplicaciones, que su organización ha creado para App Layering.
- **Secreto del cliente:** La contraseña del ID de cliente que está mediante. Si ha olvidado el secreto del cliente, puede crear uno nuevo. > **Nota:**

Cada vez que utilice una nueva suscripción y un ID de arrendatario, debe introducir un nuevo secreto de cliente. Esto se debe a que los secretos de los clientes están asociados lógicamente con los arrendatarios de Azure Government.

- **Nombre de la cuenta de almacenamiento:** Cuenta de almacenamiento de Azure Government que quiere utilizar al almacenar discos de máquinas virtuales de Azure Government. Este nombre debe cumplir con las restricciones de nomenclatura de cuentas de almacenamiento de Azure Government. Por ejemplo, el nombre de la cuenta de almacenamiento no puede contener caracteres en mayúsculas.

Debe crear una cuenta de almacenamiento a través del portal o utilizar una cuenta de almacenamiento existente que se ajuste a los siguientes criterios. La cuenta:

- No puede ser una cuenta de almacenamiento clásica.
- Ser una cuenta de almacenamiento independiente de la que se utiliza para el dispositivo. Esta nueva cuenta de almacenamiento se utiliza durante la creación de capas y la publicación de imágenes en capas.
- Debe estar en la ubicación de Azure Government donde implementará máquinas virtuales.

- Debe ser uno de los siguientes tipos:
 - Almacenamiento de información con redundancia local estándar (LRS)
 - Almacenamiento de información georredundante estándar (GRS)
 - Almacenamiento de información georredundante de acceso de lectura estándar (RAGRS)
- Se puede ubicar en cualquier grupo de recursos, siempre que la ubicación del grupo de recursos sea la misma que la ubicación de la cuenta.

Creación de máquinas para XenServer

May 9, 2024

La configuración del conector de Machine Creation for XenServer contiene la información que permite al dispositivo Citrix App Layering publicar imágenes en capas en la creación de máquinas en su entorno de XenServer. La información incluye las credenciales de usuario y la ubicación de almacenamiento.

Para publicar imágenes en capas, utilice la configuración del conector de Machine Creation for XenServer. En Configuración del conector, asegúrese de configurar una plantilla de máquina virtual. A continuación, la imagen en capas que publique estará en una máquina virtual lista para usar, la imagen se apagará y se tomará una instantánea. Puede usar la máquina virtual en su entorno de XenServer sin más modificaciones.

Cada configuración de conector está configurada para publicar imágenes en capas en una ubicación de almacenamiento específica en su entorno. Si publica en varias ubicaciones, es posible que necesite más de una configuración de conector de creación de máquinas. También puede publicar cada imagen en capas en una ubicación conveniente para el sistema que aprovisiona con la imagen publicada.

Notas:

Esta configuración de conector sirve para publicar imágenes en capas. No se pueden empaquetar capas en el entorno de creación de máquinas. Para las capas de empaquetado, utilice una [configuración de conector de XenServer](#).

No se admite un disco Personal vDisk para la creación de máquinas. Las imágenes de escritorio publicadas no son persistentes. Solo se puede utilizar un disco Personal vDisk cuando se publica en Citrix Provisioning.

Antes de comenzar

Puede usar el entorno de XenServer para crear capas y publicar imágenes en capas. Cada configuración de Connector accede a una ubicación de almacenamiento específica en el entorno de XenServer. Es posible que necesite más de una configuración de XenServer Connector para acceder a la ubicación correcta para cada propósito. Además, puede publicar cada imagen en capas en una ubicación conveniente para el sistema donde aprovisiona la imagen publicada.

XenServer utiliza una arquitectura tipo pod en la que interactúa con servidores individuales o clústeres de servidores, en lugar de con un servidor de administración central. Puede administrar los pods mediante el acceso por línea de comandos o un software de administración de GUI, como XenCenter. Instale XenCenter en el escritorio y, a continuación, podrá conectarse de forma individual a cada host independiente o a un clúster de hosts.

Uso del servicio App Layering por primera vez

Si quiere crear capas mediante una máquina virtual de XenServer, necesita un conector de XenServer en App Layering. Al publicar imágenes en capas en XenServer, también necesita una configuración de conector para cada una de las ubicaciones de publicación.

Seleccione una configuración de conector al crear una capa de aplicaciones y publicar una imagen en capas. Si necesita una configuración de conector para la tarea, puede crear una. Para hacerlo, haga clic en **Agregar configuración de conectores** en la página **Conectores**.

Información necesaria para los parámetros de la configuración del conector de Machine Creation for XenServer

Al configurar un conector para la creación de máquinas para XenServer, puede buscar el servidor, el almacén de datos y el host de XenCenter para utilizarlos en una nueva configuración.

Importante:

Los campos distinguen entre mayúsculas y minúsculas. Cualquier valor que introduzca manualmente debe coincidir con las mayúsculas y minúsculas del objeto en XenServer o, de lo contrario, la validación fallará.

- **Nombre de la configuración:** el nombre de la configuración del conector.
- **Dirección de XenServer:** nombre del host de XenServer con el que se integra el dispositivo.
- **Nombre de usuario y contraseña:** las credenciales de la cuenta que usa el dispositivo para conectarse a XenServer.
- **Usar protocolo seguro:** la configuración predeterminada que permite el cifrado SSL para el tráfico de conexión de la API entre Connector y XenServer.

- **Plantilla de máquina virtual:** la plantilla de máquina virtual que puede usar para la clonación. La lista de opciones incluye solo plantillas de máquina virtual personalizadas, en lugar de máquinas virtuales reales o cualquiera de las plantillas integradas. La plantilla seleccionada no puede tener ningún disco conectado y debe tener al menos una tarjeta de red conectada. Si la plantilla no tiene estos elementos, aparece un error al intentar validar o guardar la configuración.
- **Repositorio de almacenamiento:** el repositorio de almacenamiento del disco cargado. La lista se filtra para mostrar repositorios que pueden contener discos duros virtuales (VHD). Los repositorios ISO se filtran.
- **Utilice HTTPS para las transferencias de archivos:** cifra las transferencias de archivos de imágenes. HTTPS está seleccionado de forma predeterminada para las cargas y descargas. Puede desmarcar la casilla de verificación para aumentar el rendimiento.
- **Composición de descarga (recomendado):** permite que el proceso de empaquetado de capas o publicación de imágenes se ejecute en el servidor de hipervisor especificado. Esta función aumenta el rendimiento y permite utilizar el formato de disco VMDK y máquinas virtuales BIOS o UEFI. Con UEFI, también puedes usar Secure Boot si está habilitado en el hipervisor.
- **Repositorio de almacenamiento ISO:** repositorio para los discos que carga Offload Compositing. La lista se filtra para mostrar solo los repositorios ISO. Se admiten SMB y NFS.
- **Ruta de compartición ISO:** se rellena automáticamente para el repositorio de almacenamiento ISO seleccionado según la ruta de compartición ISO configurada. Solo para visualización.
- **Nombre de usuario del recurso compartido ISO:** nombre de usuario del recurso compartido ISO seleccionado. Solo válido para SMB ISO Share. NFS ISO Share no admite un nombre de usuario ni una contraseña.
- **Contraseña de compartición ISO:** Contraseña para el recurso compartido ISO seleccionado. Solo válido para SMB ISO Share. NFS ISO Share no admite un nombre de usuario ni una contraseña.

Cuando se selecciona Descarga de composición:

- Si proporciona una plantilla configurada para BIOS o UEFI, la máquina virtual resultante será del tipo que haya elegido.
- Si proporciona una plantilla con UEFI-Secure Boot habilitado y seleccionado, la máquina virtual resultante es UEFI-Secure Boot.

Si la opción Descargar composición no está seleccionada:

- Si proporciona una plantilla configurada para BIOS, la máquina virtual resultante es BIOS.
- Si proporciona una plantilla configurada para UEFI y cuando intenta guardar la configuración del conector, aparece un error.

Organización de máquinas virtuales

Puede organizar las máquinas virtuales de XenServer por carpeta o por etiqueta. Estas herramientas organizativas son opcionales al crear y administrar máquinas virtuales a través de XenCenter u otras herramientas. Las configuraciones del conector de XenServer no permiten especificar carpetas o etiquetas. Las máquinas virtuales creadas con el conector de XenServer, tanto las máquinas de empaquetado como la imagen en capas publicada pueden usar ambas herramientas organizativas.

Etiquetas

Si la plantilla especificada en la configuración del conector de XenServer contiene etiquetas, las etiquetas se transfieren a cualquier máquina virtual clonada a partir de esa plantilla. Por lo tanto, todas las máquinas virtuales de empaquetado o las imágenes en capas publicadas reciben las mismas etiquetas que están en la plantilla. Además, el conector de XenServer agrega tres etiquetas.

- **Unidesk:** muestra todas las máquinas virtuales creadas por el conector de XenServer, independientemente de su propósito o imagen.
- **Etiqueta de propósito:** etiqueta todas las máquinas de empaquetado con la máquina de empaquetado de App Layering. Etiqueta todas las máquinas virtuales de imágenes en capas publicadas con imágenes publicadas en App Layering.
- **Nombre de imagen/capa:** proporciona una etiqueta en todas las máquinas de empaquetado con el nombre de la capa a partir de la que se generan. Etiqueta todas las imágenes en capas publicadas con el nombre de la imagen de la plantilla.

Si usa XenCenter, puede ver las máquinas virtuales por etiqueta; para ello, seleccione **Vistas de organización** y, a continuación, seleccione **Por etiqueta**.

Carpeta

De forma predeterminada, las máquinas virtuales creadas por el conector de XenServer no se colocan en una carpeta. Si la plantilla especificada se encuentra en una carpeta, las máquinas virtuales que crea la configuración del conector se encuentran en la misma carpeta. Todas las máquinas virtuales de empaquetado y las imágenes publicadas en capas se colocan en esa misma carpeta. No hay carpetas independientes para empaquetar máquinas virtuales o imágenes en capas publicadas.

Conectividad de red de máquinas

Al crear máquinas virtuales con el conector de XenServer, se mantiene la configuración de red virtual de la plantilla de origen de la configuración del conector. No hay una opción disponible en la interfaz de usuario de configuración del conector para anular la configuración de red.

El conector de XenServer no funciona correctamente con los clústeres de XenServer. Si el host de la configuración forma parte de un clúster, debe especificar el host principal para que funcione el conector. Sin embargo, si el host principal de XenServer falla y se elige un nuevo host principal, debe actualizar la configuración de XenServer.

Crear una configuración de conector

Para escribir valores:

- Escriba los tres primeros campos Connector manualmente. Tras validar las credenciales de esos campos, puede seleccionar valores para los campos restantes en los menús desplegables.
- Para escribir valores manualmente, haga clic para poner el cursor en el campo y escriba el valor, asegurándose de que las mayúsculas y minúsculas coinciden con el valor en XenServer.
- Para seleccionar un valor de una lista desplegable, haga clic una vez para colocar el cursor en el campo. A continuación, haga clic una segunda vez para mostrar la lista de valores posibles.

Para agregar una configuración de conector

1. Haga clic en la página **Conectores**.
2. Haga clic en **Agregar configuración de conector**. Se abre un cuadro de diálogo.
3. Seleccione el **tipo de conector** para la plataforma y la ubicación en la que va a crear la capa o publicar la imagen.
4. Haga clic en **Nuevo** para abrir la página de configuración del conector.
5. Escriba el **nombre** de configuración, la dirección de XenServer, el nombre de usuario, la contraseña y la configuración de la casilla **Usar comunicaciones seguras**. Para obtener más información, consulta las definiciones de campo anteriores.
6. Haga clic en **CONECTAR** debajo de los campos de configuración de XenServer. A continuación, se habilitan los campos de **configuración de clonación de máquinas virtuales** si el nombre de usuario y la contraseña son correctos.

Nota:

Si hay un error en el certificado, aparece el siguiente mensaje de error:

```
One or more problems with the service certificate were found
. You can enable them to be ignored, or you must update the
certificate on the server.
```

Puede hacer clic en **Omitir errores de certificado y continuar**.

7. Seleccione la **plantilla de máquina virtual** requerida.

8. Seleccione el **repositorio de almacenamiento**.
9. Seleccione la configuración de **Usar HTTPS para transferencias de archivos**.
10. Seleccione la configuración para **Usar composición de descarga**.
11. Si se selecciona **Usar composición de descarga**, seleccione **Repositorio** de almacenamiento **ISO**. La **ruta de compartición ISO** se rellena automáticamente.
12. Si se selecciona un recurso compartido **ISO de SMB**, introduzca el nombre de usuario y la contraseña del recurso **ISO de SMB**.
13. Haz clic en **CONFIRMAR Y COMPLETAR**. Se muestra un resumen de la configuración.
14. Haga clic en **Guardar**. Si no se muestra ningún error, la nueva configuración del conector se guarda y se muestra en la página **Conector**.

Machine Creation for Hyper-V

July 6, 2022

Aunque no exista una configuración del conector de Machine Creation for Hyper-V, puede utilizar la configuración del conector de Hyper-V para configurar las credenciales y la ubicación de almacenamiento que el dispositivo necesita para publicar imágenes en capas en una ubicación de creación de máquinas específica dentro del entorno de MS Hyper-V.

Cada configuración de conector está configurada para acceder a una ubicación de almacenamiento específica en su entorno. Dado que necesita las imágenes en una ubicación conveniente para los sistemas que está Provisioning, existe la posibilidad de que necesite más de una configuración de conector para publicar en la creación de máquinas.

Notas:

- Esta configuración de conector es solo para publicar imágenes en capas. No puede empaquetar capas mediante esta configuración. Para empaquetar capas, utilice una configuración de conector MS Hyper-V.
- Al crear una plantilla de imagen para publicarla en Machine Creation para Hyper-V, *debe* seleccionar el tipo Sysprep **generalizado sin conexión**.
- No se admite un disco Personal vDisk para la creación de máquinas. Las imágenes de escritorio publicadas no son persistentes. Solo se puede utilizar un disco Personal vDisk al publicar en MS Hyper-V.

Para obtener más información sobre los conectores y las configuraciones de conectores, consulte [Configuración de conectores](#).

Antes de comenzar

La primera vez que cree una plantilla de imagen para publicar imágenes en capas en la creación de máquinas, debe agregar una configuración de conector de Hyper-V para esa ubicación.

Requisitos de App Layering

El agente de App Layering es necesario para utilizar un conector de creación de máquinas para Hyper-V. El agente debe ser:

- Instalado en el servidor donde quiere publicar imágenes en capas. Para obtener más información, consulte [Instalar el agente de App Layering](#) en el tema Instalación de App Layering.
- Registrado con el dispositivo de App Layering. Para obtener más información, consulte [Registro manual con el dispositivo App Layering](#) en el tema Instalación de App Layering.

Requisitos de creación de máquinas y MS Hyper-V

En esta sección se describe la información que necesita para crear un conector de Machine Creation for Hyper-V.

Plantilla de máquina virtual Antes de empezar, configure una *plantilla de máquina virtual* que la configuración del conector pueda usar para clonar una máquina virtual con la configuración de hardware deseada (memoria, CPU y configuración de vídeo). El uso de una plantilla garantiza lo siguiente:

- La imagen publicada se encuentra en una máquina virtual lista para usar.
- La imagen está apagada.
- Se toma una instantánea.

Credenciales y ubicación de MS Hyper-V La información que necesita para la configuración del conector de Hyper-V incluye:

- **Configuración de Hyper-V**
 - **Agente:** **Agente** de App Layering de la lista de agentes registrados en el dispositivo.
 - **Nombre de usuario:** **nombre** de usuario del agente.
 - **Contraseña:** Contraseña del agente.
- **Configuración de la máquina virtual**

- **VM de plantilla (opcional):** Plantilla que se puede usar para clonar una máquina virtual Hyper-V con la configuración de hardware deseada (configuración de memoria, CPU y vídeo). Puede especificar el host, el almacén de datos y la red para configurar las máquinas virtuales resultantes. La plantilla debe tener al menos una tarjeta de red conectada y no debe tener ningún disco conectado. De lo contrario, recibirá un error al intentar validar o guardar la configuración.
 - **Cantidad de CPU:** Cantidad de CPU que se utilizarán para crear una máquina de empaquetado o publicar una imagen en capas. El valor predeterminado es 4 CPU.
 - **Memoria (Mb):** Cantidad de memoria asignada para crear la máquina empaquetadora o la máquina con imágenes en capas. El valor predeterminado es 8192 Mb.
 - **Red:** Conmutador de red. Puede seleccionar de una lista de conmutadores de red conocidos por el agente.
- **Configuración de almacenamiento**
 - **Ruta remota al almacenamiento,** por ejemplo, máquinas virtuales de servidor: ruta UNC al recurso compartido de archivos que se utiliza para la creación de capas y la publicación.
 - **Ruta local al almacenamiento,** por ejemplo, C:\Virtual Machines: ubicación en la que se crean los discos y las máquinas de empaquetado. Este valor *debe* ser el mismo que la ubicación especificada en la ruta UNC.
 - **Usar la casilla Credenciales del agente:** Si se marca, las credenciales del agente se utilizan como credenciales del recurso compartido de archivos. De lo contrario, debe especificar las credenciales utilizadas para conectarse al recurso compartido de archivos.
 - **Nombre de usuario y contraseña** (si es diferente de usar las credenciales del agente): estos valores solo son necesarios si ha optado por *no* usar las credenciales del agente.
 - **Tamaño de caché de disco de capa en GB (opcional):** Cantidad de espacio de uso compartido de archivos (en gigabytes) que se utilizará para almacenar en caché los discos de capa. Un valor de:
 - * 0 inhabilita el almacenamiento en caché de capas.
 - * 1+ habilita el almacenamiento en caché de capas y especifica la cantidad de espacio para almacenar en caché los discos de capa en el recurso compartido de archivos. conservar copias de los discos de arranque y de los discos de empaquetado y volver a utilizar estos discos para crear máquinas de empaquetado. La reutilización de estos discos de arranque y discos de empaquetado reduce el tiempo que se tarda en empaquetar una capa de aplicaciones.

Crear una configuración de conector de Hyper-V para Machine Creation

Para utilizar el conector de Hyper-V para publicar en la creación de máquinas en Hyper-V:

1. Haga clic en la página **Conectores**.

2. Haga clic en **Agregar configuración de conector** para abrir un pequeño cuadro de diálogo.
3. Seleccione el tipo de conector **Microsoft Hyper-V**. A continuación, haga clic en **Nuevo** para abrir la página de configuración del conector.
4. Complete los campos de la página Configuración del conector. Para obtener orientación, consulte las definiciones de campo en la sección de requisitos anterior.
5. Haga clic en el botón **PROBAR** para comprobar que el dispositivo puede acceder a la ubicación especificada mediante las credenciales proporcionadas.
6. Haga clic en **GUARDAR** y compruebe que la nueva configuración del conector aparezca en la ficha **Conector**.

Creación de máquinas para Google Cloud

June 30, 2021

Una configuración de conector contiene las credenciales que utiliza el dispositivo para acceder a un proyecto específico en Google Cloud. Tu organización puede tener uno o varios proyectos de Google Cloud y necesitas una configuración de conector para que el dispositivo tenga acceso a cada uno de ellos.

En este artículo se describen los valores necesarios para configurar una configuración de Machine Creation for Google Cloud connector. Para obtener más información sobre las configuraciones de conectores y cómo agregarlas, consulte [Connect](#).

Antes de crear esta configuración de conector

En esta sección se explica:

- La información de la cuenta de Google Cloud necesaria para crear esta configuración de conector.
- El almacenamiento de Google Cloud que necesitas para App Layering.

Clave de cuenta de servicio y cuenta de servicio de Google Cloud requeridas

La configuración del conector de Google Cloud requiere la siguiente información.

- **Proyecto** : ID del proyecto de un proyecto de Google Cloud.
- **Archivo de clave de cuenta de servicio** : para realizar llamadas a la API como cuenta de servicio en nombre de la configuración del conector.

- **Almacenamiento:** ubicación de almacenamiento en Google Cloud para almacenar discos virtuales cargados por el conector.
- **Plantilla de instancias:** **plantilla** de máquina virtual de Google Cloud con la configuración deseada para crear una máquina virtual.
- **Tipo de disco:** tipo de [Almacenamiento de Google Cloud](#).
- **Zona:** Google Cloud Zone en la que planeas crear capas o publicar imágenes mediante la configuración del conector.

Depósito de almacenamiento de Google Cloud obligatorio

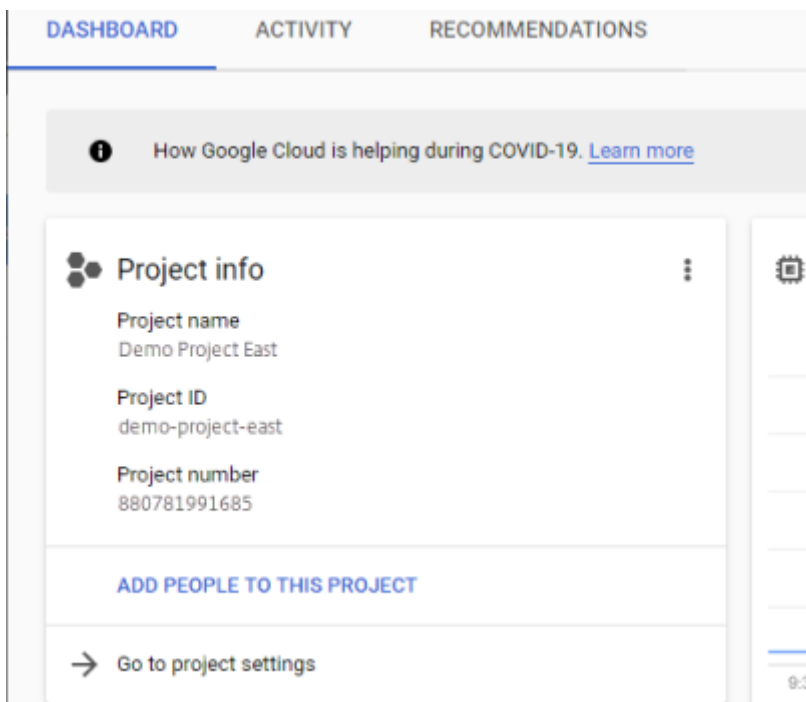
Cualquier cuenta que utilices para App Layering debe cumplir los siguientes requisitos:

- Debe estar separado del cubo de almacenamiento utilizado para el aparato.
- Debe encontrarse en la ubicación de Google Cloud en la que planea implementar máquinas virtuales.

Crear una cuenta de servicio de Google y un archivo de clave de cuenta de servicio

Utilice los siguientes procedimientos para cada proyecto de Google Cloud que desee conectar con el dispositivo App Layering.

1. Inicia sesión en **console.cloud.google.com**.
2. Seleccione el proyecto y haga clic en **Ir a la configuración del proyecto**.



3. En el panel izquierdo, **haz clic en Cuentas de servicio**.
4. En la parte superior de la página, haz clic en **+ CREAR CUENTA DE SERVICIO**.
5. Añade los detalles de tu cuenta de servicio
 - Nombre de esta cuenta de servicio: Nombre descriptivo. Por ejemplo, TestEast1
 - ID de cuenta de servicio: rellena lo que has puesto en el campo nombre, usa ese valor.
6. Haz clic en el botón **Crear**.

Agregue las funciones de su cuenta de servicio

En el cuadro **Seleccionar rol**, seleccione los roles necesarios:

- Administrador de almacenamiento
 - Administrador de procesos
 - Usuario de cuenta de servicio
1. Haga clic en el botón **Continuar**.
 2. Haz clic en el botón **Listo**. El acceso de los usuarios al rol no es necesario.

Crear un archivo de clave de cuenta de servicio

1. En el proyecto, selecciona la pestaña **Cuenta de servicio** situada a la izquierda.
2. Haz clic en los tres puntos verticales a la derecha de la cuenta de servicio para la que quieres crear el archivo clave.
3. Selecciona **Crear clave**.
4. En la ventana emergente, seleccione el botón de radio JSON y haga clic en el botón **CREAR**.
5. Cuando se le pida que guarde la clave en un archivo, introduzca el nombre de su elección o mantenga el nombre predeterminado. Vuelves a la pantalla Cuentas de servicio.
6. Haz clic en tu cuenta de servicio para comprobar que la clave está ahí.

Editar roles de cuenta de servicio

Para editar los roles:

1. Navega hasta la pantalla de la interfaz de usuario del proyecto tal como lo hacías al crear la cuenta de servicio.

2. En el menú de hamburguesas de la parte superior izquierda, expande **IAM y ADMIN** y selecciona **Administrar recursos**.
3. Seleccione su proyecto y, a la derecha, escriba la **cuenta de servicio** que desea editar en el árbol de filtros. Se muestra el nombre de la cuenta de servicio.
4. Edite cada uno de los roles para incluirlos o quitarlos de los roles y guardar los resultados.

Nota:

Si elimina todo el privilegio de la cuenta de servicio, ya no se mostrará en la página de IAM (porque la página de IAM solo muestra las cuentas con al menos un rol adjunto). Pero aparecerá en la pantalla Cuenta de servicio. Tendría que ir a la página de IAM para volver a agregar privilegios.

5. Haz clic en el botón **AÑADIR**.
6. En el panel **Agregar miembros, roles al proyecto «actual»**, en el campo **Nuevos miembros**, escriba el nombre del miembro al que desea otorgar privilegios.
7. Seleccione los roles que desea asignar al miembro y haga clic en el botón **GUARDAR**.

Creación de máquinas para Nutanix AHV (Acropolis)

May 9, 2024

La configuración del conector **AHV de Machine Creation for Nutanix** contiene las credenciales y la ubicación de almacenamiento que el dispositivo App Layering necesita para publicar imágenes en capas para la creación automática en su entorno de Nutanix AHV. Este conector no admite la creación de capas.

Antes de comenzar

Puede utilizar Machine Creation for Nutanix AHV para publicar imágenes en capas. Cada configuración de conector accede a una ubicación de almacenamiento específica en su entorno de Nutanix AHV en la que puede publicar imágenes en capas.

Es posible que necesite más de una configuración de conector AHV de Nutanix para acceder a la ubicación correcta para cada propósito. Además, es importante publicar cada imagen en capas en una ubicación conveniente para los sistemas que planea aprovisionar mediante la imagen publicada. Para obtener más información sobre los conectores y las configuraciones de conectores, consulte [Configuración de conectores](#).

Si esta es la primera vez que usa App Layering

Al publicar imágenes en capas en Nutanix AHV, necesita al menos una configuración de conector para cada ubicación de almacenamiento en la que planea publicar. Puede agregar configuraciones de conectores al crear una plantilla de imagen a partir de la que publique imágenes en capas. Si aún no tiene la configuración de conectores correcta para la tarea, puede crear una haciendo clic en **Nuevo** en la pestaña Asistente de conectores.

Información necesaria para la configuración del conector Nutanix AHV

El asistente de configuración del conector AHV de Nutanix le permite explorar el servidor, el almacén de datos y el host de Nutanix AHV para utilizarlos en una nueva configuración.

Importante

Los campos distinguen entre mayúsculas y minúsculas. Los valores que introduzca manualmente deben coincidir con las mayúsculas y minúsculas del objeto en Nutanix AHV. De lo contrario, la validación falla.

- **Nombre del conector:** nombre útil para ayudar a identificar y realizar un seguimiento de la configuración del conector AHV de Nutanix.
- **Nombre de usuario/contraseña:** credenciales que se utilizan al interactuar con el sistema Nutanix. El usuario especificado debe tener privilegios suficientes para las siguientes operaciones:
 - Operaciones de VM:
 - * clon
 - * eliminar
 - * encendido/apagado
 - * adjuntar discos virtuales
 - Operaciones de imagen:
 - * create
 - * update (también conocido como upload)
 - * eliminar
 - Discos virtuales:
 - * create
 - * conectar con máquinas virtuales
- **Permitir errores de certificado:** le permite usar el cifrado SSL para el tráfico de conexión de API entre App Layering Connector y Nutanix AHV. Este campo se borra de forma predeterminada.
- **Plantilla de máquina virtual (VM) (obligatoria):** la plantilla usada para clonar una máquina virtual con los parámetros de hardware para la creación de máquinas, incluida la memoria, las

CPU y los parámetros de vídeo. Utilice la plantilla de máquina virtual para especificar el host, el almacén de datos y la red para configurar las máquinas virtuales resultantes. Dado que no existe un concepto de “plantilla” en Nutanix, estas “plantillas” son VM reales. La versión del sistema operativo utilizada por la «plantilla» seleccionada *debe* coincidir con la versión del sistema operativo que está utilizando en las imágenes en capas. La plantilla *no* debe tener ningún disco conectado y debe tener al menos una tarjeta de red conectada. Si no lo hace, verá un error al intentar validar o guardar la configuración.

- **Contenedor de almacenamiento:** le permite seleccionar el contenedor de almacenamiento para las imágenes (discos virtuales, VHD) que se cargan y los discos virtuales resultantes que se crean a partir de esas imágenes. Al crear versiones de capas de aplicaciones y capas de SO, debemos montar el contenedor de almacenamiento como un punto de montaje NFS. El contenedor de almacenamiento seleccionado DEBE incluir el dispositivo en una lista de permitidos de clientes a los que se permite montar el contenedor de almacenamiento mediante NFS. La configuración de la lista de permitidos debe realizarse a través del producto Nutanix (ya sea su consola web o a través de sus herramientas CLI). Si el dispositivo no está correctamente permitido en la lista para el contenedor de almacenamiento seleccionado, se produce un error en la fase de validación y el error se indica con la selección del contenedor de almacenamiento.
- **Composición de descarga:** permite que el proceso de empaquetado de capas o publicación de imágenes se ejecute en el servidor Nutanix especificado. Esta función aumenta el rendimiento y permite utilizar un formato de disco nativo y máquinas virtuales BIOS o UEFI. Habilitado de forma predeterminada.

Cómo se organizan las máquinas virtuales

Nutanix no proporciona un mecanismo para organizar máquinas virtuales. Debido a esto, puede ser difícil encontrar las máquinas virtuales creadas por el dispositivo de App Layering cuando el número total de máquinas virtuales es grande. Para ayudarle a encontrar estas máquinas virtuales, se utilizan las siguientes convenciones de nomenclatura:

- **Máquinas de empaquetado** (máquinas virtuales creadas durante el proceso de creación de una capa de aplicaciones o una versión del sistema operativo)
 - El nombre de la máquina virtual comienza con el nombre de la capa que se está creando/modificando
 - Los nombres de las máquinas virtuales terminan con el siguiente texto: (Máquina de empaquetado)
- **Máquinas virtuales con imágenes en capas** (máquinas virtuales creadas como resultado de la publicación de una imagen en capas)
 - El nombre de la máquina virtual comienza con el nombre de la imagen que se publicó

- El nombre de la máquina virtual termina con el siguiente texto: (Imagen publicada)

Al ver máquinas virtuales a través de la consola web de Nutanix, puede buscar máquinas virtuales filtrando:

- “Citrix App Layering” para buscar todas las máquinas virtuales creadas por el software App Layering.
- “Citrix App Layering” para buscar todas las máquinas virtuales creadas para trabajos de administración de capas.
- “Citrix App Layering” para buscar todas las máquinas virtuales creadas para publicar una imagen en capas.
- Nombre de imagen o nombre de capa para buscar máquinas virtuales relacionadas con un trabajo de publicación de imágenes en capas específico o creación de aplicaciones o sistemas operativos.

Conectividad de red de máquinas virtuales

La configuración de red virtual de la plantilla de origen especificada en la configuración del conector de Nutanix AHV se transfiere al crear cualquier VM a través del conector de Nutanix Acropolis Hypervisor (AHV). No hay ninguna opción en la interfaz de usuario de configuración del conector para anular la configuración de red.

Crear una configuración de conector Para introducir valores:

- Los tres primeros campos Conector deben introducirse manualmente. Una vez validadas las credenciales de esos campos, puede seleccionar valores para los campos restantes en los menús desplegables.
- Para introducir valores manualmente, haga clic para colocar el cursor en el campo y escriba el valor, asegurándose de que la caja coincida con el valor del hipervisor AHV de Nutanix.
- Para seleccionar un valor de una lista desplegable, haga clic una vez para colocar el cursor en el campo y una segunda vez para mostrar la lista de valores posibles.

Para agregar una configuración de conector:

1. En el asistente para crear una capa o para agregar una versión de capa, haga clic en la ficha **Conector**.
2. Debajo de la lista de configuraciones de conectores, haga clic en el botón **Nuevo**. Esto abre un pequeño cuadro de diálogo.
3. Seleccione el tipo de conector para la plataforma y la ubicación en la que va a crear la capa o publicar la imagen. A continuación, haga clic en **Nuevo** para abrir la página de configuración del conector

4. Introduzca el *nombre* de la configuración y la dirección, el *nombre de usuario* y la *contraseña* de *Nutanix AHV* . Para obtener orientación, consulte las definiciones de campos anteriores.
5. Haga clic en el botón **Conectar** situado debajo de los campos de configuración de Nutanix AHV. El campo **Configuración de clonación de máquinas virtuales** se habilita entonces si la conexión se realiza correctamente. Los problemas de conexión se notifican en el módulo de configuración del conector. Si se han encontrado errores en el certificado del servidor, aparece el botón **Omitir errores de certificado y continuar** .
6. Seleccione la plantilla de máquina virtual.
7. Seleccione el repositorio de almacenamiento.
8. Haga clic en **Confirmar y completar**. Si no hay errores, se muestra una página de resumen.
9. Haga clic en **Guardar**. Compruebe que la nueva configuración del conector aparezca en la página **Conector**.

Machine Creation for vSphere

July 6, 2022

Una configuración del conector de Machine Creation for vSphere contiene las credenciales y la ubicación de almacenamiento necesarias para publicar imágenes en capas en la creación de máquinas en el entorno de vSphere.

Puede publicar imágenes en capas en la creación de máquinas que se ejecute en un entorno de vSphere mediante la configuración del conector de Machine Creation for vSphere. En la configuración del conector, asegúrese de configurar una plantilla de máquina virtual para que la imagen en capas que publique esté en una máquina virtual lista para usar, se cierre la imagen y se tome una instantánea. Puede utilizar la máquina virtual en su entorno de Horizon sin más modificaciones.

Cada configuración de conector está configurada para publicar imágenes en capas en una ubicación de almacenamiento específica del entorno, por lo que es posible que necesite más de una configuración de conector si se publica en varias ubicaciones. Además, es posible que quiera publicar cada imagen en capas en una ubicación conveniente para el sistema que está Provisioning con la imagen publicada. Para obtener más información sobre conectores y configuraciones de conectores, consulte [Conectar](#).

Notas:

Esta configuración de conector sirve para publicar imágenes en capas. No se pueden empaquetar capas en el entorno.

La creación de máquinas no admite discos personales vDisk. Las imágenes de escritorio publicadas no son persistentes. Actualmente, los discos vDisk solo se pueden usar cuando se publican

en Citrix Provisioning.

Antes de comenzar

La primera vez que cree una plantilla de imagen para publicar imágenes en capas en una ubicación del entorno, cree una configuración de conector para esa ubicación.

Información necesaria para la configuración de este Conector

La configuración de un conector para Machine Creation for vSphere le permite buscar vCenter Server, Data Store y Host para usarlos en una nueva configuración.

Importante:

Los campos distinguen mayúsculas y minúsculas, por lo que cualquier valor que introduzca manualmente debe coincidir con el caso del objeto de su entorno, o la validación falla.

- **Nombre:** un nombre útil para ayudar a identificar la configuración de este conector.
- **vCenter Server:** el nombre del servidor vSphere con el que se integra el dispositivo.
- **Nombre de usuario de vCenter:** el nombre de usuario de la cuenta que el dispositivo usa para conectarse a vSphere.
- **Contraseña de vCenter:** la contraseña de la cuenta que utiliza el dispositivo para conectarse a vSphere.
- **Nombre del centro de datos:** el nombre del centro de datos de vSphere en el que el dispositivo crea y recupera las máquinas virtuales.
- **Plantilla de máquina virtual (recomendada, necesaria para máquinas virtuales UEFI):** plantilla que se puede usar para clonar una máquina virtual con la configuración de hardware para la creación de máquinas, incluida la configuración de memoria, CPU y vídeo. Puede especificar el host, el almacén de datos y la red para configurar las máquinas virtuales resultantes. La lista de opciones contiene solo plantillas de VM personalizadas, en lugar de máquinas virtuales reales o cualquiera de las plantillas integradas. La versión del sistema operativo utilizada por la plantilla seleccionada debe coincidir con la versión del sistema operativo que se utiliza para publicar imágenes en capas. La plantilla no debe tener ningún disco conectado y debe tener al menos una tarjeta de red conectada. Si no lo hace, verá un error al intentar validar o guardar la configuración.
- **Nombre del almacén de datos:** el nombre de vSphere DataStore en el que el dispositivo crea máquinas virtuales.
- **Nombre de host ESX:** el nombre del host de vSphere ESX en el que el dispositivo crea máquinas virtuales.
- **Nombre de la red:** el nombre de la red de vSphere en la que el dispositivo crea las máquinas virtuales.

- **Nombre de la carpeta de la máquina virtual:** el nombre de la carpeta de vSphere en la que el dispositivo crea las máquinas virtuales.
- **Descargar composición: permite que** el proceso de creación de paquetes de capas o publicación de imágenes se ejecute en el servidor especificado. Esta función aumenta el rendimiento y permite utilizar el formato de disco VMDK y máquinas virtuales BIOS o UEFI. Cuando se selecciona Descarga de composición:
 - Si *no* proporciona una plantilla de máquina virtual, la máquina virtual utilizará el BIOS de forma predeterminada.
 - Si proporciona una plantilla configurada para BIOS o UEFI, la máquina virtual resultante es el tipo elegido.
Si no se selecciona Descargar composición:
 - Si **no** proporciona una plantilla, la máquina virtual se establece de forma predeterminada en BIOS.
 - Si proporciona una plantilla configurada para BIOS, la máquina virtual resultante es BIOS.
 - Si proporciona una plantilla configurada para UEFI, la máquina no arranca y aparece una pantalla azul.

Crear una configuración de conector

Para introducir valores:

- Los tres primeros campos de vCenter deben introducirse manualmente. Una vez validadas las credenciales de esos campos, puede seleccionar valores para los campos restantes en los menús desplegables.
- Para introducir valores manualmente: haga clic para colocar el cursor en el campo y escriba el valor.
- Para seleccionar un valor de una lista desplegable: Haga clic una vez para colocar el cursor en el campo y una segunda vez para elegir entre una lista de valores posibles.

Para agregar una nueva configuración de conector

1. Haga clic en la página **Conectores**.
2. Haga clic en **Agregar configuración de conector**. Esto abre un pequeño cuadro de diálogo.
3. Seleccione el tipo de conector para la plataforma y la ubicación en la que está creando la capa o publicando la imagen. A continuación, haga clic en Nuevo para abrir la página Configuración del conector.
4. Introduzca el nombre de configuración y vCenter Server, el nombre de usuario de vCenter y la contraseña de vCenter. Para obtener orientación, consulte las definiciones de campos anteriores.

5. Haga clic en el botón **COMPROBAR CREDENCIALES** debajo de los campos de vCenter. A continuación, el campo del centro de datos se habilita con una lista de centros de datos disponibles.
6. Seleccione el centro de datos y los menús desplegados restantes estarán habilitados.
7. (Recomendado) Seleccione una máquina virtual para utilizarla como plantilla. Aunque una plantilla de VM es opcional, se recomienda.
8. Complete los campos restantes y haga clic en el botón **PROBAR** para comprobar que el dispositivo puede acceder a la ubicación especificada mediante las credenciales proporcionadas.
9. Haga clic en **Guardar**. Verifique que la nueva configuración del conector aparezca en la página **Conectores**.

Configuración de scripts (opcional, función avanzada)

Al crear una configuración de conector, puede configurar un script opcional de PowerShell en cualquier máquina Windows que ejecute un agente de App Layering. Estos scripts deben almacenarse en el mismo equipo en el que está instalado el Agente de App Layering y solo se ejecutan después de una implementación correcta de una imagen en capas. Algunas variables preestablecidas están disponibles para permitir que los scripts sean reutilizables con diferentes imágenes de plantilla y configuraciones de conectores diferentes. Estas variables también contienen información necesaria para identificar la máquina virtual creada como parte de la imagen en capas publicada en vSphere.

La ejecución de estos scripts no afectará al resultado del trabajo de publicación, y el progreso de los comandos ejecutados en el script no es visible. Los registros del conector de vSphere contienen la salida del script que se ejecutó.

Configurar un script

Recuerde que este paso es opcional. Si quiere que se ejecute un script cada vez que se publique una imagen en capas, siga estos pasos mediante los valores descritos en las secciones siguientes.

1. Complete y guarde la configuración del conector como se describe anteriormente.

Nota:

Antes de seleccionar la página **Configuración de script**, debe guardar (o descartar) cualquier modificación en los parámetros de configuración del conector.

2. Si el menú de **navegación** de la izquierda no está abierto, selecciónelo y haga clic en **Configuración de scripts** para abrir la página **Ruta del script**.
3. Complete los campos obligatorios con los valores que se detallan aquí y, a continuación, haga clic en **Guardar**.

Campos de configuración de scripts

Habilitar script: Marque esta casilla para activar los campos restantes. Esto le permite introducir un script que se ejecuta cada vez que se publica una imagen en capas.

Agente de scripts: La máquina del agente en la que se encuentran los scripts.

Nombre de usuario (opcional): El nombre de usuario que se va a suplantar al ejecutar el script. Esto se puede utilizar para garantizar que el script se ejecuta en el contexto de un usuario que tiene los derechos/permisos necesarios para realizar las operaciones en el script.

Contraseña (opcional): La contraseña del nombre de usuario especificado.

Ruta de script: Una ruta completa y un nombre de archivo en la máquina agente en la que reside el archivo de script.

Otros valores de configuración de scripts

Variables de PowerShell Cuando se ejecuta el script, se establecen las siguientes variables y se pueden utilizar en el script de PowerShell:

Valor	Se aplica a tipos de conectores	Valor determinado por el código	Descripción
connectorCfgName	Todas	Código común	Nombre de la configuración del conector a la que está asociada la configuración del script.
imageName	Todas	Código común	El nombre de la plantilla de imagen en capas que se utilizó para compilar/publicar la imagen en capas.

Valor	Se aplica a tipos de conectores	Valor determinado por el código	Descripción
osType	Todas	Código común	El tipo de sistema operativo de la imagen en capas publicada. Puede ser uno de los siguientes valores: Windows7; Windows764; Windows200864; Windows201264; Windows10; Windows1064
virtualInfrastructureServer	Todas	Código del conector de vSphere	El servidor vCenter especificado en la configuración del conector.
vmName	Todas	Código del conector de vSphere	Nombre de la máquina virtual que se creó.
vmId	Todas	Código del conector de vSphere	El ID de máquina virtual tomado de la máquina virtual (es decir, "vm-12345")
vmUuid	Todas	Código del conector de vSphere	El UUID de la máquina virtual.

Suplantación de usuario

El Agente de App Layering, que se ejecuta como un servicio en un equipo Windows, se ejecuta en la cuenta del sistema local o en la cuenta de red. Cualquiera de estas cuentas puede tener algunos privilegios especiales, pero a menudo están restringidos al ejecutar comandos específicos o ver archivos en el sistema de archivos. Por lo tanto, App Layering le da la opción de agregar un usuario de dominio y una contraseña que se pueden usar para "suplantar" a un usuario. Esto significa que el script se ejecuta como si ese usuario hubiera iniciado sesión en el sistema, de modo que cualquier comando o dato sea accesible sujeto a esos derechos y permisos de usuario. Si no se introduce un nombre de usuario o una contraseña, el script se ejecuta mediante la cuenta en la que el servicio está configurado para ejecutarse.

Directiva de ejecución de scripts Los requisitos de la directiva de ejecución de scripts dependen de usted. Si tiene intención de ejecutar scripts sin firmar, debe configurar la directiva de ejecución en una de las directivas más indulgentes. Sin embargo, si firma sus propios scripts, puede optar por utilizar una directiva de ejecución más restrictiva.

MS Azure

December 21, 2022

Importante:

Esta configuración del conector de Azure ahora está en desuso y solo está disponible durante un tiempo limitado. Para las conexiones de Azure, utilice la nueva configuración del conector de [implementaciones de Azure](#).

Al crear capas en un entorno de Azure, utilice una configuración de conector de MS Azure. En este artículo se describen los campos incluidos en la **configuración del conector de Azure**. Para obtener más información sobre las configuraciones de conectores y cómo agregar otros nuevos, consulte [Configuraciones de conectores](#).

Una configuración de conector contiene las credenciales que utiliza el dispositivo para acceder a una ubicación específica de Azure. Su organización puede tener una cuenta de Azure y varias ubicaciones de almacenamiento. Necesita una configuración de conector para que el dispositivo tenga acceso a cada ubicación de almacenamiento.

Nota:

Este conector se usa para publicar capas. **No** utilice este conector para publicar plantillas.

Antes de crear una configuración de Azure Connector

En esta sección se explica:

- La información de la cuenta de Azure necesaria para crear esta configuración de conector.
- El almacenamiento de Azure que necesita para App Layering.
- Los servidores con los que se comunica el dispositivo.

Información necesaria de la cuenta de Azure

La configuración del conector de Azure requiere la siguiente información.

Azure Connector Configuration [Help](#)

Enter your Azure credentials and storage account to define this Connector Configuration. You may optionally specify a premium storage account for storing Azure virtual machine disks. For more information and steps to find your Azure credentials, click Help.

Name:

Subscription ID:

Tenant ID:

Client ID:

Client Secret:

Standard Storage Account:

Premium Storage Account (optional):

- **Nombre:** Nombre que se utiliza para una nueva configuración de conector.
- **ID de suscripción:** Para implementar máquinas virtuales Azure, su organización debe tener un ID de suscripción.
- **ID de arrendatario:** Instancia de Azure Active Directory, este GUID identifica la instancia dedicada de Azure Active Directory (AD) de su organización.
- **ID de cliente:** Identificador del registro de aplicaciones, que su organización ha creado para App Layering.
- **Secreto de cliente:** La contraseña del ID de cliente que está utilizando. Si ha olvidado el secreto del cliente, puede crear uno. **Nota:** Los secretos de cliente están asociados lógicamente con los arrendatarios de Azure, por lo que cada vez que utilice una nueva suscripción e ID de arrendatario, debe usar un nuevo secreto de cliente.

- **Almacenamiento estándar de Azure (obligatorio):** cuenta de almacenamiento para máquinas virtuales Azure (archivos VHD), el archivo de plantilla que utiliza para implementar máquinas virtuales Azure y los archivos de diagnóstico de arranque de las máquinas virtuales Azure. Si especifica Almacenamiento **Premium**, que es *opcional*, las máquinas virtuales se almacenan allí y los archivos de diagnóstico de plantilla y arranque permanecen en el almacenamiento estándar.

La cuenta de almacenamiento ya debe haberse creado en Azure Portal y el nombre que escriba debe coincidir con el nombre del portal. Para obtener más información, consulta [Configurar una o varias cuentas de almacenamiento necesarias](#) a continuación.

- **Almacenamiento premium (opcional):** almacenamiento adicional opcional para máquinas virtuales Azure (archivos VHD). El almacenamiento Premium solo admite blobs de página y no se puede usar para almacenar el archivo de plantilla para implementar máquinas virtuales de Azure o los archivos de diagnóstico de arranque para esas máquinas virtuales. Cuando especifica una cuenta de almacenamiento premium, los tamaños de máquina virtual disponibles se limitan a los que admiten almacenamiento premium.

La cuenta de almacenamiento ya debe haberse creado en Azure Portal y el nombre que escriba debe coincidir con el nombre del portal. Para obtener más información, consulta [Configurar una o varias cuentas de almacenamiento necesarias](#) a continuación.

Cuenta de almacenamiento de Azure requerida

Cualquier cuenta que utilices para App Layering debe cumplir los siguientes requisitos:

- No debe ser una cuenta de almacenamiento clásica.
- Debe ser independiente de la cuenta de almacenamiento utilizada para el dispositivo.
- Debe estar en la ubicación de Azure donde planea implementar máquinas virtuales.
- Se puede ubicar en cualquier grupo de recursos, siempre que la ubicación del grupo de recursos sea la misma que la ubicación de la cuenta.

Cuenta de almacenamiento estándar requerida Se requiere uno de los siguientes tipos de cuentas de almacenamiento estándar de Azure para crear una configuración de conector.

- Almacenamiento de información con redundancia local estándar (LRS)
- Almacenamiento de información georredundante estándar (GRS)
- Almacenamiento de información georredundante de acceso de lectura estándar (RAGRS)

Al crear el **almacenamiento estándar** necesario, active **Blob Public Access** para esta cuenta. De lo contrario, los intentos de publicar imágenes fallan con el error:

```
1 "A failure occurred while creating a storage container in the Azure storage account: Public access is not permitted on this storage account."
```

Cuenta de almacenamiento premium Además de la **cuenta estándar** requerida, puedes usar el **almacenamiento Premium** para almacenar los discos de tu máquina virtual de App Layering. Al crear el **almacenamiento Premium** opcional, no se requiere **acceso público a blob**.

Servidores con los que el dispositivo se comunica

Mediante este conector, el dispositivo se comunica con los siguientes servidores:

- management.azure.com
- login.windows.net
- management.core.windows.net
- portal.azure.com/#create/Microsoft.Template/uri
- blob.core.windows.net

El dispositivo requiere conexiones de red con estos servidores.

Configurar suscripciones de Azure

Utilice los siguientes procedimientos para cada suscripción de Azure que quiera conectar con el dispositivo App Layering.

Configurar y obtener las credenciales de Azure

Para recuperar credenciales de Azure al agregar una configuración de Azure Connector:

- Identifique su ID de suscripción de Azure.
- Crear un registro de aplicaciones en Azure Active Directory.
- Obtenga el ID de arrendatario, el ID de cliente y el secreto de cliente de Azure del registro de aplicaciones.
- Cree una cuenta de almacenamiento, o use una existente, dentro de la suscripción.

Identificar el ID de suscripción de Azure correcto

1. Vaya al [portal de Azure](#).
2. Haga clic en **Suscripciones** y busca la suscripción que necesitas en la lista.
3. Seleccione y copie el ID de suscripción y péguelo en el campo ID de suscripción de configuración del conector.

Crear un registro de aplicación para la suscripción de Azure Puede usar una suscripción de Azure para varias configuraciones de conectores de Azure. Cada suscripción de Azure que quiera usar para las configuraciones del conector de App Layering requiere un registro de aplicaciones.

Para crear un registro de aplicación:

1. Inicie sesión en el [portal de Azure](#).
2. Haga clic en **Azure Active Directory**.
Si Azure Active Directory no aparece en la lista, haga clic en **Más servicios** para mostrar más opciones.
3. En la parte izquierda, debajo de **Administrar**, selecciona **Registros de aplicaciones**.
4. En la parte superior de la página, haga clic en **Nuevo registro**.
Aparece un formulario.
5. En el campo **Nombre**, escriba un nombre descriptivo, como “Acceso a Citrix App Layering”.
6. En **Tipos de cuentas compatibles**, seleccione **Cuentas en este directorio organizativo únicamente (soloMi empresa: Arrendatario único)**.
7. En **URL de redirección**, escriba `https://myapp.com/auth`.
8. Haga clic en **Registrar**.
9. En la lista de registros de aplicaciones, haga clic en el nuevo registro de aplicaciones que creó en el procedimiento anterior.
10. En la nueva ventana que aparece, el ID de aplicación aparece cerca de la parte superior. Introduzca este valor en el cuadro **ID de cliente** de la configuración del conector que va a crear.
11. Desplácese hacia la derecha para ver las propiedades de la aplicación, incluidos el nombre para mostrar, el ID de aplicación y otros valores.
12. Copie el valor de **ID de directorio (arrendatario)** y péguelo en el campo **ID de arrendatario** de la configuración del conector.
13. En la columna izquierda, debajo de **Administrar**, haga clic en **Certificados y secretos**.
14. Agregue un secreto de cliente para la aplicación App Layering, con una descripción como “App Layering Key 1”.
15. Escriba el valor del nuevo **secreto de cliente** en la configuración del conector.

Nota:

Esta clave no aparece de nuevo después de cerrar esta ventana. Esta clave es información confidencial. Trate la clave como una contraseña que permite el acceso administrativo a su suscripción de Azure. Abra la configuración del registro de aplicaciones que creó en **Azure Active Directory > Registros de aplicaciones > [nombre que acaba de introducir]**

> **Configuración > Propiedades.**

16. Vuelva a Azure Home y haga clic en **Suscripciones**. Si **las suscripciones** no aparecen en la lista, haga clic en **Más servicios** para localizarla.
17. Haga clic en la suscripción que está usando para este conector.
18. En el panel izquierdo, haga clic en **Control de acceso (IAM)**.
19. En la barra superior del panel de control de acceso, haga clic en **Agregar** y seleccione **Agregar asignación de funciones**.
20. El formulario **Agregar asignación de funciones** aparece a la derecha. Haga clic en el menú desplegable de **Función** y selecciona **Colaborador**.
21. En el campo **Seleccionar**, escriba “Acceso a Citrix App Layering” o utilice el nombre que ha introducido para el registro de la aplicación.
22. Haga clic en el botón **Guardar** en la parte inferior del formulario.

Ahora ha configurado un registro de aplicaciones de Azure que tiene acceso de lectura/escritura a su suscripción de Azure.

Configurar una o más cuentas de almacenamiento necesarias Las cuentas de almacenamiento de Azure son donde el software de App Layering almacena todas las imágenes importadas y publicadas en Azure (discos duros virtuales o VHD), junto con el archivo de plantilla que utiliza para implementar máquinas virtuales de Azure, y los archivos de diagnóstico de arranque para esas máquinas.

Puede usar una cuenta de almacenamiento existente, si cumple estos requisitos:

- No es una cuenta de almacenamiento clásica.
- Está en la misma suscripción utilizada en la configuración del conector.

En la configuración del conector de Azure de App Layering, introduzca el nombre de la cuenta de almacenamiento en el campo **Cuenta de almacenamiento estándar**.

Si no tiene una cuenta de almacenamiento, cree una cuenta de almacenamiento **estándar**. Las configuraciones de conectores requieren una cuenta estándar, aunque también puede especificar una segunda cuenta de almacenamiento que sea premium.

1. En la página principal de Azure, haga clic en **Cuentas de almacenamiento**.
2. En la ventana **Cuentas de almacenamiento**, haga clic en **Agregar**.
3. En el campo **Suscripción**, seleccione la suscripción que está usando.
4. En el campo **Grupo de recursos**, seleccione **Crear nuevo** e introduzca un nombre similar al nombre de la cuenta de almacenamiento.
5. En el campo **Nombre de la cuenta de almacenamiento**, introduce un nombre fácil de recordar.

6. Seleccione la **ubicación**.
7. En el campo **Rendimiento**, si la ubicación elegida es la única para esta configuración de conector, seleccione **Estándar**. De lo contrario, elija el tipo que mejor se adapte a sus necesidades.
8. En el campo **Tipo de cuenta**, seleccione **General purpose v2** o **General purpose v1**.
9. En el campo **Replicación**, seleccione el tipo que necesita.
10. Para el **nivel de acceso (predeterminado)**, seleccione **Caliente** o **Frío**.
11. Haga clic en **Siguiente: redes** y seleccione el método de conectividad.
12. Complete las opciones restantes en Redes, Avanzadas y Etiquetas.
13. Seleccione **Review + Create**.
14. Por último, introduzca el nuevo **nombre de la cuenta de almacenamiento** en la configuración del conector que va a crear.

Qué hacer si su Azure Client Secret se pierde Puede generar un nuevo secreto de cliente de Azure mediante los **certificados y secretos**. Para obtener más información, consulte los pasos de la sección *Crear un registro de aplicación para cada suscripción de Azure* que aparece anteriormente en este artículo.

Agregar una configuración de conector

Cuando los requisitos estén listos, cree una configuración de Azure Connector:

1. Haga clic en la página **Conectores**.
2. Haga clic en **Agregar configuración de conector**.
3. En el cuadro de diálogo que se abre, seleccione el tipo de conector para la plataforma y la ubicación en la que está creando la capa o publicando la imagen en capas. A continuación, haga clic en **Nuevo** para abrir la página **Configuración del conector**.
4. Complete los campos de la página **Configuración del conector**. Para obtener orientación, consulte las definiciones de campo.
5. Haga clic en el botón **PROBAR** para comprobar que el dispositivo puede acceder a la ubicación especificada mediante las credenciales proporcionadas.
6. Haga clic en **Guardar**. La nueva configuración del conector aparece en la ficha Conector

Estructura de datos de Azure (referencia)

La estructura de datos de Azure es la siguiente:

Arrendatario

- ID de arrendatario
- Registro de aplicaciones

- ID de cliente
- Secreto del cliente
- Subscription
- ID de suscripción
 - Cuenta de almacenamiento
 - * Nombre de la cuenta de almacenamiento

Donde:

- *Tenant* es la instancia de Azure Active Directory que los usuarios y las aplicaciones pueden usar para acceder a Azure. El ID de arrendatario identifica cada arrendatario. Un arrendatario puede tener acceso a una o varias suscripciones de Azure.
- El arrendatario de Azure Active Directory contiene dos tipos de cuentas.
 - Una *cuenta de usuario* para iniciar sesión en el portal de Azure (portal.azure.com).
 - El *registro de una aplicación* para acceder a la suscripción tiene un ID de cliente.
 - * El ID de cliente tiene un secreto de cliente, en lugar de una contraseña.
 - * Los usuarios pueden generar el secreto del cliente y eliminarlo.
- Una suscripción de Azure contiene todo lo que se puede crear en Azure, excepto las cuentas de usuario.
- Una suscripción contiene cuentas de almacenamiento. Una cuenta de almacenamiento es donde se almacenan los VHD de App Layering. El nombre de la cuenta de almacenamiento identifica la ubicación.

MS Azure Government

July 6, 2022

Al crear capas en Azure Government, use una configuración de conector de MS Azure Government. Este artículo describe los campos incluidos en la configuración del conector. Para obtener más información sobre los conectores de App Layering, consulte [Configuración de conectores](#).

Una configuración de conector contiene las credenciales que utiliza el dispositivo para acceder a una ubicación específica de Azure Government. Su organización puede tener una cuenta de Azure Government y varias ubicaciones de almacenamiento. Necesita una configuración de conector para que el dispositivo tenga acceso a cada ubicación de almacenamiento.

Antes de crear una configuración de conector de Azure Government

En esta sección se explica:

- Información de la cuenta de Azure Government necesaria para crear esta configuración de conector.
- El almacenamiento de Azure Government que necesita para App Layering.
- Los servidores con los que se comunica el dispositivo.

Información necesaria de la cuenta de Azure

El conector de Azure Government necesita la misma información que el conector de Azure.

Azure Connector Configuration [Help](#)

Enter your Azure credentials and storage account to define this Connector Configuration. You may optionally specify a premium storage account for storing Azure virtual machine disks. For more information and steps to find your Azure credentials, click Help.

Name:

Subscription ID:

Tenant ID:

Client ID:

Client Secret:

Standard Storage Account:

Premium Storage Account (optional):

- **Nombre:** Nombre que se utiliza para una nueva configuración de conector.
- **ID de suscripción:** Para implementar máquinas virtuales Azure, su organización debe tener un ID de suscripción.
- **ID de arrendatario:** Instancia de Azure Active Directory, este GUID identifica la instancia dedicada de Azure Active Directory (AD) de su organización.
- **ID de cliente:** Identificador del registro de aplicaciones, que su organización ha creado para App Layering.
- **Secreto de cliente:** La contraseña del ID de cliente que está utilizando. Si ha olvidado el secreto del cliente, puede crear uno nuevo. **Nota:** Los secretos de cliente están asociados lógicamente con los arrendatarios de Azure, por lo que cada vez que utilice una nueva suscripción e ID de arrendatario, debe usar un nuevo secreto de cliente.
- **Almacenamiento estándar de Azure (obligatorio):** una cuenta de almacenamiento para máquinas virtuales de Azure (archivos VHD), el archivo de plantilla que se usa para implementar máquinas virtuales de Azure y los archivos de diagnóstico de arranque de esas máquinas. Cuando especifica el almacenamiento **Premium**, que es *opcional*, las máquinas virtuales se almacenan allí y la plantilla y los archivos de diagnóstico de arranque permanecen en el almacenamiento estándar.

La cuenta de almacenamiento ya debe haberse creado en el portal de Azure Government y el nombre que escriba debe coincidir con el nombre del portal. Para obtener más información, consulta [Configurar las cuentas de almacenamiento necesarias](#) a continuación.

- **Almacenamiento premium (opcional):** más almacenamiento para las máquinas virtuales de Azure (archivos VHD). El almacenamiento premium solo admite blobs de página. No puede usar almacenamiento premium para almacenar el archivo de plantilla para implementar máquinas virtuales de Azure, ni los archivos de diagnóstico de arranque para esas máquinas virtuales. Cuando especifica una cuenta de almacenamiento premium, los tamaños de máquina virtual disponibles se limitan a los que admiten almacenamiento premium.

La cuenta de almacenamiento ya debe haberse creado en el portal de Azure Government y el nombre que escriba debe coincidir con el nombre del portal. Para obtener más información, consulte [Configurar las cuentas de almacenamiento necesarias](#) más adelante en este artículo.

Cuenta de almacenamiento de Azure gubernamental requerida

Cualquier cuenta que utilices para App Layering debe cumplir los siguientes requisitos:

- No debe ser una cuenta de almacenamiento clásica.
- Debe ser independiente de la cuenta de almacenamiento utilizada para el dispositivo.

- Debe estar en la ubicación de Azure Government donde planea implementar máquinas virtuales.
- Se puede ubicar en cualquier grupo de recursos, siempre que la ubicación del grupo de recursos sea la misma que la ubicación de la cuenta.

Cuenta de almacenamiento estándar requerida Se requiere uno de los siguientes tipos de cuentas de almacenamiento estándar de Azure Government) para crear una configuración de conector.

- Almacenamiento de información con redundancia local estándar (LRS)
- Almacenamiento de información georredundante estándar (GRS)
- Almacenamiento de información georredundante de acceso de lectura estándar (RAGRS)

Al crear el **almacenamiento estándar** necesario, active **Blob Public Access** para esta cuenta. De lo contrario, los intentos de publicar imágenes fallan con el error:

```
1 "A failure occurred while creating a storage container in the Azure storage account: Public access is not permitted on this storage account."
```

Cuenta de almacenamiento premium Además de la cuenta Standard necesaria, puede usar el almacenamiento Premium para almacenar los discos de su máquina virtual App Layering.

Servidores con los que el dispositivo se comunica

Mediante este conector, el dispositivo se comunica con los siguientes servidores:

- login.microsoftonline.us
- management.usgovcloudapi.net
- management.core.us.govcloudapi.net
- portal.azure.us/#create/Microsoft.Template/uri/
- blob.core.us.govcloudapi.net

El dispositivo requiere conexiones de red con estos servidores.

Configurar su suscripción de Azure Government

Utilice los siguientes procedimientos para cada suscripción de Azure Government que quiera conectar con el dispositivo App Layering.

Configurar y obtener las credenciales de Azure Government

Al agregar una nueva configuración del conector de MS Azure Government, recupere las credenciales de Azure Government de la siguiente manera:

- Identifique su ID de suscripción de Azure Government
- Cree un registro de aplicaciones en Azure Government Active Directory.
- Obtenga el ID de arrendatario, el ID de cliente y el secreto de cliente de Azure Government del registro de aplicaciones.
- Cree una nueva cuenta de almacenamiento o use una existente dentro de la suscripción.

Identificar el ID de suscripción de Azure Government

1. Vaya al [portal de Azure Government](#).
2. Haga clic en **Suscripciones** y busca la suscripción que necesitas en la lista.
3. Seleccione y copie el ID de suscripción y péguelo en el campo **ID de suscripción** de configuración del conector.

Crear un registro de aplicación para cada suscripción de Azure Government

Puede usar una suscripción de Azure Government para varias configuraciones de conectores de Azure. Cada suscripción que quiera utilizar para las configuraciones del conector de App Layering requiere un registro de aplicaciones.

Para crear un registro de aplicación:

1. Inicie sesión en el [portal Azure Government](#).
2. Haga clic en **Azure Active Directory**.
Si Azure Active Directory no aparece en la lista, haga clic en **Más servicios** y busque Azure Government Active Directory.
3. En la parte izquierda, debajo de **Administrar**, selecciona **Registros de aplicaciones**.
4. En la parte superior de la página, haga clic en **Nuevo registro**.
Aparece un formulario.
5. En el campo **Nombre**, escriba un nombre descriptivo, como “Acceso a Citrix App Layering”.
6. En **Tipos de cuentas compatibles**, seleccione **Cuentas en este directorio organizativo únicamente (soloMi empresa: Arrendatario único)**.
7. En **URL de redireccionamiento**, escriba <https://myapp.com/auth>.
8. Haga clic en **Registrar**.

9. En la lista de registros de aplicaciones, haga clic en el nuevo registro de aplicaciones que creó en el procedimiento anterior.
10. En la nueva ventana que aparece, el ID de aplicación aparece cerca de la parte superior. Introduzca este valor en el cuadro **ID de cliente** de la configuración del conector que va a crear.
11. Desplácese hacia la derecha para ver las propiedades de la aplicación, incluidos el nombre para mostrar, el ID de aplicación y otros valores.
12. Copie el valor de **ID de directorio (arrendatario)** y péguelo en el campo **ID de arrendatario** de la configuración del conector.
13. En la columna izquierda, debajo de **Administrar**, haga clic en **Certificados y secretos**.
14. Agregue un nuevo secreto de cliente para la aplicación App Layering, con una descripción como “App Layering Key 1”.
15. Escriba el valor del nuevo **secreto de cliente** en la configuración del conector.

Nota:

Esta clave no aparece de nuevo después de cerrar esta ventana. Esta clave es información confidencial. Trate la clave como una contraseña que permite el acceso administrativo a su suscripción de Azure Government. Abra la configuración del registro de aplicaciones que acaba de crear en **Azure Government Active Directory > Registros de aplicaciones > [nombre que acaba de escribir] > Configuración > Propiedades**.

16. Vuelva a Azure Home y haga clic en **Suscripciones**. Si **las suscripciones** no aparecen en la lista, haga clic en **Más servicios** para localizarla.
17. Haga clic en la suscripción que está usando para este conector.
18. En el panel izquierdo, haga clic en **Control de acceso (IAM)**.
19. En la barra superior del panel de control de acceso, haga clic en **Agregar** y seleccione **Agregar asignación de funciones**.
20. El formulario **Agregar asignación de funciones** aparece a la derecha. Haga clic en el menú desplegable de **Función** y selecciona **Colaborador**.
21. En el campo **Seleccionar**, escriba “Acceso a Citrix App Layering” o utilice el nombre que ha introducido para el registro de la aplicación.
22. Haga clic en el botón **Guardar** en la parte inferior del formulario.

Ahora ha configurado un registro de aplicación de Azure Government que tiene acceso de lectura/escritura a su suscripción de Azure Government.

Configurar las cuentas de almacenamiento necesarias

Las cuentas de almacenamiento de Azure Government son donde el software de App Layering almacena todas las imágenes importadas y publicadas en Azure Government (discos duros virtuales o VHD), junto con el archivo de plantilla que se utiliza para implementar máquinas virtuales de Azure Government y los archivos de diagnóstico de inicio para esas máquinas.

Puede usar una cuenta de almacenamiento existente. Debe cumplir estos requisitos:

- No es una cuenta de almacenamiento clásica.
- Está en la misma suscripción utilizada en la configuración del conector.

En la configuración del conector de Azure de App Layering, introduzca el nombre de la cuenta de almacenamiento en el campo **Cuenta de almacenamiento estándar**.

Si no tiene una cuenta de almacenamiento, cree una cuenta de almacenamiento **estándar**. Las configuraciones de conectores requieren una cuenta estándar, aunque también puede especificar una segunda cuenta de almacenamiento que sea premium.

1. En la página principal de Azure, haga clic en **Cuentas de almacenamiento**.
2. En la ventana **Cuentas de almacenamiento**, haga clic en **Agregar**.
3. En el campo **Suscripción**, seleccione la suscripción que está usando.
4. En el campo **Grupo de recursos**, seleccione **Crear nuevo** e introduzca un nombre similar al nombre de la cuenta de almacenamiento.
5. En el campo **Nombre de cuenta de almacenamiento**, introduzca un nombre que pueda recordar.
6. Seleccione la **ubicación**.
7. En el campo **Rendimiento**, si esta es la única ubicación de almacenamiento para esta configuración de conector, seleccione **Estándar**. De lo contrario, elija el tipo que mejor se adapte a sus necesidades.
8. En el campo **Tipo de cuenta**, seleccione **General purpose v2** o **General purpose v1**.
9. En el campo **Replicación**, seleccione el tipo que necesita.
10. Para el **nivel de acceso (predeterminado)**, seleccione **Caliente** o **Frío**.
11. Haga clic en **Siguiente: redes** y seleccione el método de conectividad.
12. Complete las opciones restantes en Redes, Avanzadas y Etiquetas.
13. Seleccione **Review + Create**.
14. Por último, introduzca el nuevo **nombre de la cuenta de almacenamiento** en la configuración del conector que va a crear.

Qué hacer si se pierde el secreto de cliente de Azure Government Puede generar un nuevo secreto de cliente de Azure mediante los **certificados y secretos**. Para obtener más información, consulte los pasos de la sección *Crear un registro de aplicación para cada suscripción de Azure* que aparece

anteriormente en este artículo.

Agregar una configuración de conector

Cuando todos los requisitos estén listos, cree una configuración del conector de Azure Government:

1. Haga clic en la página **Conectores**.
2. Haga clic en **Agregar configuración de conectores** para abrir un cuadro de diálogo.
3. Seleccione el tipo de conector para la plataforma y la ubicación en la que está creando la capa o publicando la imagen. A continuación, haga clic en **Nuevo** para abrir la página **Configuración del conector**.
4. Complete los campos de la página **Configuración del conector**. Para obtener orientación, consulte las definiciones de campo.
5. Haga clic en el botón **PROBAR** para comprobar que el dispositivo puede acceder a la ubicación especificada mediante las credenciales proporcionadas.
6. Haga clic en **Guardar**. La nueva configuración del conector aparece en la ficha Conector

Estructura de datos de Azure Government (referencia)

La estructura de datos de Azure Government es la siguiente:

Arrendatario

- ID de arrendatario
- Registro de aplicaciones
 - ID de cliente
 - Secreto del cliente
- Suscripción
- ID de suscripción
 - Cuenta de almacenamiento
 - * Nombre de la cuenta de almacenamiento

Donde:

- *Tenant* es la instancia de Active Directory de Azure Government que los usuarios y las aplicaciones pueden usar para acceder a Azure Government. El arrendatario se identifica mediante su ID de arrendatario. Un arrendatario puede tener acceso a una o más suscripciones de Azure Government.
- El arrendatario de Azure Government Active Directory contiene dos tipos de cuentas.

- Una *cuenta de usuario* para iniciar sesión en el portal de Azure Government (portal.azure.us).
- El *registro de una aplicación* para acceder a la suscripción tiene un ID de cliente.
 - * El ID de cliente tiene un secreto de cliente, en lugar de una contraseña.
 - * Los usuarios pueden generar el secreto del cliente y eliminarlo.
- Una suscripción de Azure Government contiene todo lo que se puede crear en Azure Government, excepto las cuentas de usuario.
- Una suscripción contiene cuentas de almacenamiento. Aquí es donde se almacenan los VHD de App Layering. Se identifica mediante un nombre de cuenta de almacenamiento.

MS Hyper-V

July 6, 2022

Una configuración de conector MS-Hyper-V incluye las credenciales y la ubicación de almacenamiento que el dispositivo necesita para conectarse a Hyper-V e identifica las propiedades que se van a asociar al disco vDisk.

Puede seleccionar un conector de Hyper-V para importar el sistema operativo, crear otras capas o publicar imágenes en capas. Cada configuración de conector se establece para acceder a una ubicación de almacenamiento mediante una cuenta específica.

El conector de Hyper-V utiliza el Servicio de transferencia inteligente en segundo plano (BITS) de Microsoft para copiar discos desde y hacia el dispositivo. Con BITS, el dispositivo informa del progreso como un porcentaje completado y el conector ya no requiere un recurso compartido CIFS.

El conector de Hyper-V incluye una casilla **de verificación de composición de descarga** que permite que el empaquetado de capas y la publicación de imágenes se realicen en el servidor Hyper-V, en lugar de hacerlo en el dispositivo App Layering. La composición de descarga aumenta considerablemente la velocidad del empaquetado de capas y la publicación de imágenes. También automatiza la finalización de capas y permite crear capas y publicar imágenes como máquinas Hyper-V Generation 2 en discos VHD o VHDX.

Para obtener más información sobre los conectores y las configuraciones de conectores en general, consulte [Configuraciones de conectores](#).

Antes de comenzar

La primera vez que cree una plantilla de imagen para publicar imágenes en capas en su entorno Microsoft Hyper-V, debe agregar una nueva configuración de conector de Hyper-V para esa ubicación.

Requisitos de Hyper-V

Puede utilizar una configuración de conector de Hyper-V que facilita la conexión a una ubicación en el entorno Microsoft Hyper-V.

La información que necesita para la configuración del conector de Hyper-V incluye:

- **Configuración de Hyper-V**

- **Agente:** agente de App Layering de la lista de agentes registrados en el dispositivo. El agente se ejecuta bajo la cuenta de equipo para el equipo en el que se ejecuta.

- **Configuración de la máquina virtual**

- **VM de plantilla (opcional):** Plantilla que se puede usar para clonar una máquina virtual Hyper-V con la configuración de hardware deseada (configuración de memoria, CPU y vídeo). Puede especificar el host, el data store y la red para configurar las máquinas virtuales resultantes. La plantilla debe tener al menos una tarjeta de red conectada y no debe tener ningún disco conectado. De lo contrario, recibirá un error al intentar validar o guardar la configuración.
- **Cantidad de CPU:** Cantidad de CPU que se utilizarán para crear una máquina de empaquetado o publicar una imagen en capas. El valor predeterminado es 4 CPU.
- **Memoria (Mbs):** Cantidad de memoria asignada para crear la máquina empaquetadora o la máquina con imágenes en capas. El valor predeterminado es 8192 Mb.
- **Red:** Conmutador de red. Puede seleccionar de una lista de conmutadores de red conocidos por el agente.
- **Generación:** Las máquinas de generación 1 son compatibles en todos los casos. Las máquinas de segunda generación solo se admiten cuando se selecciona la opción Descargar composición.
- **Formato de disco:** Las máquinas de primera generación admiten VHD o VHDX. Solo VHDX es compatible con máquinas de generación 2.

Nota:

El formato de disco VHDX requiere la **composición de descarga**, incluso en máquinas de primera generación.

- **Descarga de composición:** permite que el proceso de creación de paquetes de capas o publicación de imágenes se ejecute en el servidor Hyper-V especificado. Esta función aumenta el rendimiento y permite utilizar el formato de disco VHDX y las máquinas virtuales de generación 2. Con UEFI, también puede usar **Secure Boot** si está habilitado en la VM.

Cuando se selecciona Descarga de composición:

- Si no proporciona una plantilla de máquina virtual, la máquina virtual utilizará el BIOS de forma predeterminada.
- Si proporciona una plantilla configurada para BIOS o UEFI, la máquina virtual resultante es el tipo elegido.
- Si proporciona una plantilla con UEFI-Secure Boot habilitado y seleccionado, la máquina virtual resultante es UEFI-Secure Boot.

Cuando la composición de descarga no está seleccionada:

- Si no proporciona una plantilla, la máquina virtual es BIOS de forma predeterminada.
- Si proporciona una plantilla configurada para BIOS, la máquina virtual resultante es BIOS.
- Si proporciona una plantilla configurada para UEFI, la máquina no puede arrancar y da como resultado una pantalla azul. (La composición de descarga es necesaria para UEFI.)

• Configuración de almacenamiento

- **Ruta al almacenamiento, por ejemplo: C:\Virtual Machines:** Ruta de la ubicación local o remota en la que el software App Layering crea discos de capas, máquinas de empaquetado y discos de imágenes en capas. Este valor:
 - * Debe ser la misma que la ubicación especificada en la ruta de acceso UNC.
 - * No puede ser una unidad asignada.
- **Tamaño de caché de disco de capa en GB (opcional):** Cantidad de espacio de uso compartido de archivos (en gigabytes) que se utilizará para almacenar en caché los discos de capa. Un valor de:
 - * 0 inhabilita el almacenamiento en caché de capas.
 - * 1+ habilita el almacenamiento en caché de capas y especifica la cantidad de espacio para almacenar en caché los discos de capa en el recurso compartido de archivos. Las copias de los discos de arranque y de los discos de empaquetado se almacenan y luego se vuelven a utilizar siempre que sea posible para reducir el tiempo necesario para empaquetar una capa de aplicación.

Requisitos de App Layering

El agente de App Layering es necesario para usar un conector de Hyper-V. El agente de App Layering debe ser:

- Instalado en el servidor Microsoft Hyper-V donde quiere crear capas o publicar imágenes en capas. Para obtener más información, consulte [Instalar el agente de App Layering](#) en el tema Instalación de App Layering.
- Registrado con el dispositivo de App Layering. Para obtener más información, consulte [Registro manual con el dispositivo App Layering](#) en el tema Instalación de App Layering.

Crear una configuración de conector de Hyper-V

Para utilizar el conector de Hyper-V para la creación de capas o la publicación, haga lo siguiente:

1. Haga clic en la página **Conectores**.
2. Haga clic en **Agregar configuración de conector**. Esto abre un pequeño cuadro de diálogo.
3. Seleccione el tipo de conector **Microsoft Hyper-V**. A continuación, haga clic en **Nuevo** para abrir la página Configuración del conector.
4. Complete los campos de la página Configuración del conector. Para obtener instrucciones, consulte las definiciones de campos en la sección de requisitos de Hyper-V anterior.
5. Haga clic en el botón **PROBAR** para comprobar que el dispositivo puede acceder a la ubicación especificada mediante las credenciales proporcionadas.
6. Haga clic en **GUARDAR**. La nueva configuración del conector debe aparecer ahora en la ficha Conector.

Errores de HTTPS y certificados

De forma predeterminada, HTTPS está desactivado y se ignoran los errores de certificado, ya que el certificado autofirmado que viene con el dispositivo conmutaría por error HTTPS. Al cargar su propio certificado, puede configurar el conector para que use HTTPS y deje de ignorar los errores de certificado.

Si quiere habilitar HTTPS para Hyper-V

si quiere habilitar HTTPS para Hyper-V, modifique la configuración para activar HTTPS y para ignorar los errores de certificado en el archivo config.json.

1. Abra el archivo config.json del conector de Hyper-V:
`/usr/local/lib/node_modules/unidesk-hyperv-connector/config.json`
2. Establezca **useHttpsFileTransfer** en true:
“useHttpsFileTransfer”: true
3. Establezca **ignoreCertificateErrors** en false:
“ignoreCertificateErrors”: false
4. Reinicie el conector de Hyper-V.

Errores certificados

Una vez que los errores de certificado ya no se ignoran, recibirá el siguiente error si el certificado caduca:

- ```
1 Failed copying file to D:\path\file.vhdx. The certificate authority is
 invalid or incorrect.
2 The error occurred while the remote file was being processed.
```

## Nutanix AHV (Acropolis)

May 9, 2024

La configuración de un conector AHV de Nutanix contiene las credenciales y el contenedor de almacenamiento que el dispositivo necesita para conectarse a Nutanix Acropolis.

Puede utilizar esta configuración de conector para acceder a una ubicación específica en su entorno de Nutanix cuando:

- Empaquetar capas como parte de la creación de una capa de plataforma o aplicación, o como parte de agregar una versión a una capa.
- Publicar imágenes en capas en Nutanix.

### Antes de comenzar

Puede usar su entorno de Nutanix Acropolis para crear capas y publicar imágenes en capas. Cada configuración de conector accede a un contenedor de almacenamiento específico en su entorno de Nutanix Acropolis donde puede crear sus capas o publicar imágenes en capas.

Necesita más de una configuración de conector de Nutanix Acropolis para acceder al contenedor correcto para cada propósito. Además, es importante publicar cada imagen en capas en un contenedor al que puedan acceder cómodamente los sistemas a los que va a aprovisionar con la imagen publicada. Para obtener más información sobre los conectores y las configuraciones de conectores, consulte [Configuración de conectores](#).

### Especificar la consola de Nutanix Prism Elements

App Layering usa la consola web de Prism Elements y no es compatible con la consola de Prism Central.

#### **Importante:**

Al usar conectores de Nutanix, App Layering requiere acceso NFS directo a los hosts para que funcione correctamente. En versiones anteriores de Nutanix AHV (5.6 y 5.7), este acceso NFS directo a los hosts no se permitía si se registraba un host o clúster de Prism Element en Prism Central.



Asegúrese de que la configuración de Nutanix permita este acceso. Para obtener más información sobre este problema en varias versiones de Nutanix, consulte [La adición de versiones de capa con Nutanix falla con el error: No se pudo ejecutar el script](#)

Al configurar el conector de Nutanix, asegúrese de introducir la **URL** de la consola de Prism Elements.

**Error que recibe si se especifica Prism Central en el conector** Si se utiliza Prism Central en la configuración del conector, recibirá el error “Error interno 500”.

### **Agregue el dispositivo Citrix App Layering a la lista de permitidos de Nutanix**

Asegúrese de que el dispositivo se ha agregado a su lista de permisos de Nutanix para que pueda acceder a los contenedores de almacenamiento adecuados, según sea necesario. Esto se puede lograr configurando los parámetros del sistema de archivos y de la lista de permitidos a nivel de contenedor. Para obtener más información sobre cómo añadir una lista de permitidos con Nutanix, consulte la documentación de Nutanix.

### **Información necesaria para los ajustes de configuración del conector de Acropolis**

La configuración del conector de Nutanix le permite definir las credenciales y el contenedor que se utilizarán para una nueva configuración.

#### **Importante:**

Los campos distinguen entre mayúsculas y minúsculas. Cualquier valor que introduzca manualmente debe coincidir con las mayúsculas y minúsculas del objeto en Nutanix o, de lo contrario, la validación fallará.

- **Nombre de configuración del conector:** nombre útil para ayudar a identificar esta configuración de conector.
- **Dirección de la consola web (Prism):** el nombre de host (que se puede resolver mediante DNS) o la dirección IP de la consola web de Prism. Esta dirección es la misma que usa para acceder a la consola web de Nutanix Prism.
- **Nombre de usuario/contraseña:** credenciales que se utilizan al interactuar con el sistema Nutanix. El usuario especificado debe tener privilegios suficientes para las siguientes operaciones:
  - Operaciones de VM:
    - \* clon
    - \* eliminar
    - \* encendido/apagado

- \* adjuntar discos virtuales
- Operaciones de imagen:
  - \* create
  - \* update (también conocido como upload)
  - \* eliminar
- Discos virtuales:
  - \* create
  - \* conectar con máquinas virtuales
- **Plantilla de máquina virtual (recomendada):** plantilla de máquina virtual que se puede usar para clonar una máquina virtual con la configuración de hardware de Nutanix, incluida la configuración de memoria, CPU y vídeo. Puede especificar el host, el almacén de datos y la red para configurar las máquinas virtuales resultantes. Como no existe el concepto de «plantilla» en Nutanix, estas «plantillas» son máquinas virtuales reales. La versión del sistema operativo utilizada por la “plantilla” seleccionada debe coincidir con la versión del sistema operativo que está usando para crear capas o publicar imágenes en capas. La plantilla no debe tener ningún disco conectado y debe tener al menos una tarjeta de red conectada. Si no lo hace, verá un error al intentar validar o guardar la configuración.
- **Contenedor de almacenamiento:** le permite seleccionar el contenedor de almacenamiento para las imágenes (discos virtuales, VHD) que se cargan y los discos virtuales resultantes que se crean a partir de esas imágenes. Al crear capas de aplicaciones y versiones de capas de sistema operativo, monte el contenedor de almacenamiento como un punto de montaje de NFS. Configure la **lista de permitidos** mediante la consola web de Nutanix o las herramientas de la CLI de Nutanix. Establezca la lista de permitidos para el clúster y todos los contenedores de almacenamiento del clúster, incluso los que no esté utilizando.

**Nota:** Si el dispositivo no está en la lista de permitidos para el contenedor de almacenamiento seleccionado, se produce un error en la fase de validación y el error se indica con la selección del contenedor de almacenamiento.
- **Tamaño de la caché de disco de capa en GB (opcional):** especifica el tamaño de la caché permitido para cada capa.
- **Composición de descarga:** permite que el proceso de empaquetado de capas o publicación de imágenes se ejecute en el servidor Nutanix especificado. Esta función aumenta el rendimiento y permite utilizar un formato de disco nativo y máquinas virtuales BIOS o UEFI. Esto está habilitado de forma predeterminada.
- **Tamaño de la caché de empaquetado en GB (recomendado):** cantidad de espacio de tamaño de caché (en GB) que se utilizará para el empaquetado. Acepte el valor recomendado o modifíquelo.

## Cómo se organizan las máquinas virtuales

Nutanix no proporciona un mecanismo para organizar máquinas virtuales. Debido a esto, puede resultar difícil encontrar las máquinas virtuales creadas por el dispositivo cuando el número total de máquinas virtuales es grande. Para ayudarle a encontrar estas máquinas virtuales, se utilizan las siguientes convenciones de nomenclatura:

- **Máquinas de empaquetado** (máquinas virtuales creadas durante el proceso de creación de una capa de aplicaciones o una versión del sistema operativo)
  - El nombre de la máquina virtual comienza con el nombre de la capa que se está creando/modificando
  - Los nombres de las máquinas virtuales terminan con el siguiente texto: (Máquina de empaquetado)
- **Máquinas virtuales con imágenes en capas** (máquinas virtuales creadas como resultado de la publicación de una imagen en capas)
  - El nombre de la máquina virtual comienza con el nombre de la imagen que se publicó
  - El nombre de la máquina virtual termina con el siguiente texto: (Imagen publicada)

Al ver máquinas virtuales a través de la consola web de Nutanix, puede buscar máquinas virtuales filtrando:

- “Citrix App Layering” para buscar todas las máquinas virtuales creadas por el servicio App Layering.
- “Citrix App Layering Packaging Machine” para buscar todas las máquinas virtuales creadas para trabajos de administración de capas.
- “Imagen publicada en Citrix App Layering” para buscar todas las máquinas virtuales creadas para publicar una imagen en capas.
- Nombre de imagen o nombre de capa para buscar máquinas virtuales relacionadas con un trabajo de publicación de imágenes en capas específico o creación de aplicaciones o sistemas operativos.

## Conectividad de red de máquinas virtuales

La configuración de red virtual de la plantilla de origen especificada en la configuración del conector de Nutanix AHV se traspasará al crear cualquier VM a través del conector de Nutanix Acropolis Hypervisor (AHV). No hay ninguna opción en la interfaz de usuario de configuración del conector para anular la configuración de red.

## Crear una configuración de conector

Para introducir valores:

- Debe introducir manualmente los tres primeros campos del conector. Una vez validadas las credenciales de esos campos, puede seleccionar valores para los campos restantes en los menús desplegables.
- Para introducir valores manualmente, haga clic para poner el cursor en el campo y escriba el valor, asegurándose de que el caso coincide con el valor en Acropolis.
- Para seleccionar un valor de una lista desplegable, haga clic una vez para colocar el cursor en el campo y una segunda vez para mostrar la lista de valores posibles.

## Para agregar una configuración de conector

1. Inicie sesión en la consola de administración como administrador.
2. Seleccione **Conectores > Agregar configuración de conector**.
3. Seleccione **Nutanix AHV** en el menú desplegable **Tipo** de conector y haga clic en **Nuevo**. Esto abre la configuración del conector.
4. Introduzca el **Nombre** de configuración y la Dirección de Acropolis, el Nombre de usuario y la Contraseña. Para obtener orientación, consulte las definiciones de campos anteriores.
5. Haga clic en el botón **Conectar** situado debajo del campo Configuración de Acropolis. El campo **Configuración de clonación de máquinas virtuales** se habilita entonces si la conexión se realiza correctamente. Los problemas de conexión se notifican en el módulo de configuración del conector. Si se han encontrado errores en el certificado del servidor, aparece el botón **Omitir errores de certificado y continuar**.
6. Seleccione la plantilla de máquina virtual.
7. Seleccione el repositorio de almacenamiento.
8. Haga clic en **Confirmar y completar**. Si no hay errores, se muestra una página de resumen.
9. Haga clic en **Guardar**. Verifique que la nueva configuración del conector aparezca en la página **Conectores**.

## VMware vSphere

May 30, 2023

Una configuración del conector de vSphere contiene las credenciales y la ubicación de almacenamiento que el dispositivo necesita para conectarse a vSphere. Utilice el conector de vSphere para empaquetar capas y publicar imágenes en VMware vSphere o VMware Cloud en AWS.

## Antes de comenzar

Puede utilizar el entorno de vSphere para crear capas y publicar imágenes en capas. Cada configuración de conector tiene acceso a una ubicación de almacenamiento específica.

Para facilitar el Provisioning del sistema, puede publicar imágenes en capas en más de una ubicación del hipervisor. Para publicar en más de una ubicación, cree una configuración de conector para cada ubicación. Para obtener más información sobre conectores y configuraciones de conectores, consulte [Conectar](#).

La cuenta de vCenter que use para el conector debe tener los mismos permisos en un centro de datos que se enumeran en el artículo de instalación del [dispositivo de App Layering](#).

Cuando se usa vSphere como hipervisor para Citrix Provisioning, se recomienda usar la misma plantilla de máquina virtual de vSphere, en la configuración del conector de vSphere, para crear capas como lo hace para crear los dispositivos de destino en Citrix Provisioning. Esta práctica garantiza que la imagen publicada y los dispositivos de destino tengan las mismas especificaciones de máquina virtual de referencia.

## Si esta es la primera vez que usa App Layering

Si es la primera vez que utiliza App Layering y quiere crear capas con una máquina virtual vSphere, necesita un conector de vSphere. Si también publica imágenes en capas en vSphere, también puede crear una configuración de conector para cada una de sus ubicaciones de publicación.

Al crear una capa y publicar una imagen en capas, puede seleccionar una configuración de conector. Si aún no tiene la configuración de conectores correcta para la tarea, puede crear una haciendo clic en **Agregar configuración de conectores** en la página **Conectores**.

## Controladores virtuales

Puede utilizar la controladora SAS LSI Logic predeterminada o una controladora SCSI paravirtual de VMware.

Para usar el Controller LSI Logic SAS predeterminado, simplemente selecciónelo para la máquina virtual de la capa y asegúrese de que todas las capas usen el mismo Controller.

Para utilizar un Controller SCSI paravirtual de VMware, necesita una VM Plantilla preexistente con un Controller SCSI Paravirtual de VMware y sin ningún disco.

**Para utilizar una capa de SO LSI existente con una Controller SCSI Paravirtual de VMware** Si tiene una capa de SO con un Controller SAS LSI Logic y quiere usarlo con un Controller SCSI Paravirtual de VMware, puede utilizar cualquiera de los siguientes enfoques:

- Agregue una versión a la capa del sistema operativo mediante un conector de VMware vSphere con una plantilla de VM LSI Logic SAS. Cuando se cree la máquina de empaquetado, siga los pasos que se indican a continuación para que la capa del sistema operativo Paravirtual esté habilitada.
- Agregue una nueva capa de plataforma con una capa de SO LSI y un conector de plataforma con una plantilla de VM LSI Logic SAS. Cuando se cree la máquina de empaquetado, siga los pasos que se indican a continuación para activar la capa de plataforma Paravirtual.

### Nota:

Los siguientes cambios se deben realizar en la capa del sistema operativo y en la capa de plataforma.

Cuando la máquina de empaquetado de su enfoque elegido esté lista:

1. Inicie sesión en la máquina virtual y apáguela.
2. En vSphere Web Client, abra la página **Modificar configuración** de la máquina de empaquetado.
3. Agregue una nueva controladora SCSI; para ello, seleccione **Controlador SCSI** en el menú **Nuevo dispositivo** y haga clic en **Agregar**.
4. Expanda la sección **Nueva controladora SCSI** que se agregó y establezca **Cambiar tipo** en **VMware Paravirtual**.
5. Agregue un disco duro nuevo; para ello, seleccione **Nuevo disco duro** en el menú **Nuevo dispositivo** y haga clic en **Agregar**.
6. Expanda la sección Nuevo disco duro y establezca los siguientes parámetros:
  - Tamaño: 1 GB
  - Provisiónamiento de discos: provisionamiento ligero
  - Nodo de dispositivo virtual: nuevo bus predeterminado de Controller SCSI
7. Haga clic en **Aceptar**.
8. Instale los controladores Paravirtual encendiendo la máquina de empaque, iniciando sesión y, a continuación, apagando.
9. En vSphere Web Client, abra la página **Modificar configuración** de la máquina de empaquetado.
10. Quite tanto el disco duro como el Controller paravirtual que agregó anteriormente en este procedimiento.
11. Encienda la máquina de empaquetado, inicie sesión y haga clic **en Apagar para finalizar**.

Una vez que termine de crear la capa, puede usarla para crear una imagen con un Controller Paravirtual.

## Información necesaria para la configuración de vSphere Connector

La configuración de un conector para vSphere le permite buscar vCenter Server, el almacén de datos y el host para usarlos en una nueva configuración.

### Importante:

Los campos distinguen mayúsculas y minúsculas, por lo que los valores que introduzca manualmente deben coincidir con las mayúsculas y minúsculas del objeto en vSphere, o la validación no se puede realizar

- **Nombre de configuración del conector:** Un nombre útil para ayudar a identificar y rastrear esta configuración de conector.
- **vCenter Server:** el nombre del servidor vSphere con el que se integra el dispositivo.
- **Nombre de usuario de vCenter:** el nombre de usuario de la cuenta que el dispositivo usa para conectarse a vSphere.
- **Contraseña de vCenter:** la contraseña de la cuenta que el dispositivo usa para conectarse a vSphere.
- **Nombre del centro de datos:** el nombre del centro de datos de vSphere en el que el dispositivo de App Layering crea y recupera máquinas virtuales.
- **Tamaño de la memoria caché de paquetes en GB (recomendado):** el tamaño de la caché de disco que App Layering usa al crear capas. Si deja vacío el tamaño o lo establece en 0, App Layering no utiliza una caché de disco. Si especifica un tamaño, App Layering usa una caché de disco de hasta este tamaño para guardar copias de los discos de arranque y los discos de empaquetado, y los reutiliza para crear máquinas de empaquetado. La reutilización de estos discos de arranque y de empaquetado reduce el tiempo que se tarda en empaquetar una capa de aplicaciones.
- **Plantilla de máquina virtual:** (opcional) Plantilla de máquina virtual que clona una máquina virtual con la configuración de hardware de VMware, incluidas la memoria, las CPU y la configuración de vídeo. Esta configuración le permite especificar el host, el almacén de datos y la red para configurar las máquinas virtuales resultantes.

### Importante:

Al publicar en VMware Cloud, se requiere una **plantilla de máquina virtual de VMware** (no una plantilla de máquina virtual normal) para que la red de la máquina virtual funcione correctamente.

Al seleccionar una máquina virtual de plantilla:

- Responda **Sí** al mensaje que le pide que actualice la configuración, pero **no** cambie la red.

- Asegúrese de que la versión del sistema operativo que utiliza la plantilla seleccionada coincida con la versión del sistema operativo que utiliza para crear capas o publicar imágenes en capas.
- La plantilla no debe tener ningún disco conectado y debe tener al menos una tarjeta de red conectada. De lo contrario, recibirá un error al intentar validar o guardar la configuración.
- **Nombre de ESXHost:** El nombre del host de vSphereESX en el que el dispositivo crea y recupera máquinas virtuales.
- **Nombre del almacén de datos:** El nombre del almacén de datos de vSphere en el que el dispositivo crea y recupera máquinas virtuales.
- **Nombre de red:** El nombre de la red de vSphere en la que el dispositivo crea y recupera máquinas virtuales.
- **Nombre de la carpeta de la máquina virtual:** El nombre de la carpeta de vSphere en la que el dispositivo crea y recupera máquinas virtuales.
- **Compositing de descarga:** Permite que el proceso de publicación de imágenes o empaquetado de capas se ejecute en el servidor vSphere especificado. Esta función aumenta el rendimiento y permite utilizar el formato de disco VMDK y máquinas virtuales BIOS o UEFI. Con UEFI, también puede usar **Arranque seguro** si está habilitado en la máquina virtual.

### Importante:

Cuando se usa una configuración de conector de vSphere con VMware Cloud y un almacén de datos de vSAN 7.0 Update 2 (o posterior), se debe seleccionar **Compositing de descarga**.

Cuando se selecciona Descarga de composición:

- Si *no* proporciona una plantilla de máquina virtual, la máquina virtual utilizará el BIOS de forma predeterminada.
- Si proporciona una plantilla configurada para BIOS o UEFI, la máquina virtual resultante es el tipo elegido.
- Si proporciona una plantilla con UEFI-Secure Boot habilitado y seleccionado, la máquina virtual resultante es UEFI-Secure Boot.

Si la opción Descargar composición no está seleccionada:

- Si no proporciona una plantilla, la máquina virtual es BIOS de forma predeterminada.
- Si proporciona una plantilla configurada para BIOS, la máquina virtual resultante es BIOS.
- Si proporciona una plantilla configurada para UEFI, la máquina no puede arrancar y da como resultado una pantalla azul. (La composición de descarga es necesaria para UEFI.)



### **Privilegios requeridos para la función de administrador del cliente vSphere del conector**

Establezca los privilegios de VMware requeridos por el administrador de vSphere Client para que coincidan con los permisos del [dispositivo de App Layering](#).

Una vez que haya establecido los permisos, compruébelos haciendo clic en **Guardar** en el módulo de resumen de configuración Create Connector.

### **Crear una configuración de conector**

Para introducir valores:

- Los tres primeros campos de vCenter deben introducirse manualmente. Una vez validadas las credenciales de esos campos, puede seleccionar valores para los campos restantes en los menús desplegables.
- Para introducir valores manualmente, haga clic para colocar el cursor en el campo y escriba el valor, asegurándose de que la caja coincida con el valor de vCenter.
- Para seleccionar un valor de una lista desplegable, haga clic una vez para colocar el cursor en el campo y mostrar la lista de valores posibles.

### **Para agregar una nueva configuración de conector**

1. Haga clic en la página **Conectores**.
2. Haga clic en **Agregar configuración de conector**. Se abre un cuadro de diálogo.
3. Seleccione el tipo de conector para la plataforma y la ubicación en la que va a crear la capa o publicar la imagen. A continuación, haga clic en **Nuevo** para abrir la página de configuración del conector.
4. Introduzca el *nombre* de la configuración y el *servidor de vCenter*, el *nombre de usuario de vCenter* y la *contraseña de vCenter*. Para obtener información, consulte las definiciones de campos anteriores.
5. Haga clic en el botón **Conectar** situado debajo de los campos de vCenter. A continuación, el campo del centro de datos se habilita con una lista de centros de datos disponibles.
6. Seleccione el centro de datos, habilitando las listas desplegables restantes.
7. Complete los campos restantes y haga clic en el botón **PROBAR** para comprobar que App Layering puede acceder a la ubicación especificada con las credenciales proporcionadas.
8. Haga clic en **Guardar**. Verifique que la nueva configuración del conector aparezca en la página **Conectores**.

## Configuración de scripts (opcional, función avanzada)

Al crear una configuración de conector, puede configurar un script opcional de PowerShell en cualquier máquina Windows que ejecute un agente de App Layering, el mismo agente utilizado en el servidor de Citrix Provisioning. Los scripts deben almacenarse en la máquina en la que está instalado el agente de App Layering y solo se ejecutarán después de una implementación correcta de una imagen en capas.

Algunas variables preestablecidas están disponibles para permitir que los scripts sean reutilizables con diferentes imágenes de plantilla y configuraciones de conectores diferentes. Estas variables también contienen información necesaria para identificar la máquina virtual creada como parte de la imagen en capas publicada en vSphere.

La ejecución de los scripts afecta al resultado del trabajo de publicación y el progreso del script no está visible. Los registros del conector de vSphere contienen la salida del script después de ejecutarse.

### Configurar un script

Recuerde que este es un procedimiento opcional. Si quiere que se ejecute un script cada vez que se publique una imagen en capas, siga estos pasos mediante los valores descritos en las secciones siguientes.

1. Complete y guarde la configuración del conector tal y como se ha descrito anteriormente.

#### Nota:

Antes de seleccionar la página **Configuración de scripts**, debe guardar (o descartar) cualquier modificación en los valores de configuración del conector,

2. Si el menú de navegación de la izquierda no está abierto, selecciónelo y, a continuación, haga clic en **Configuración del script** para abrir la página Ruta del script.
3. Complete los campos obligatorios con los valores que se detallan aquí y haga clic en **Guardar**.

### Campos de configuración de scripts

- **Habilitar guión:** seleccione esta casilla de verificación para habilitar los campos restantes. Esto le permite introducir un script que se ejecuta cada vez que se publica una imagen en capas.
- **Agente de scripts:** La máquina del agente en la que se encuentran y se ejecutan los scripts.
- **Nombre de usuario (opcional):** el nombre de usuario que se va a *suplantar* al ejecutar el script. Esto se puede utilizar para garantizar que el script se ejecute en el contexto de un usuario que tenga los permisos para realizar las operaciones del script.
- **Contraseña (opcional):** la contraseña del nombre de usuario especificado.

- **Ruta:** Una ruta completa y un nombre de archivo en la máquina agente donde permanece el archivo de script.

### Otros valores de configuración de scripts

Cuando se ejecuta el script, se establecen las siguientes variables y se pueden utilizar en el script de PowerShell:

| Valor                       | Se aplica a tipos de conectores | Valor determinado por el código | Descripción                                                                                                                                                                                                                  |
|-----------------------------|---------------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| connectorCfgName            | Todas                           | Código común                    | Este es el nombre de la configuración del conector a la que se asocia la configuración del script.                                                                                                                           |
| imageName                   | Todas                           | Código común                    | Este es el nombre de la plantilla de imagen en capas que se utilizó para compilar/publicar la imagen en capas.                                                                                                               |
| osType                      | Todas                           | Código común                    | Tipo de sistema operativo de la imagen en capas publicada. Puede ser uno de los siguientes valores:<br>Windows7;<br>Windows764;<br>Windows8;<br>Windows864;<br>Windows200864;<br>Windows201264;<br>Windows10;<br>Windows1064 |
| virtualInfrastructureServer | Todas                           | Código del conector de vSphere  | El servidor vCenter especificado en la configuración del conector.                                                                                                                                                           |
| vmName                      | Todas                           | Código del conector de vSphere  | El nombre de la máquina virtual.                                                                                                                                                                                             |

| Valor  | Se aplica a tipos de conectores | Valor determinado por el código | Descripción                                                            |
|--------|---------------------------------|---------------------------------|------------------------------------------------------------------------|
| vmId   | Todas                           | Código del conector de vSphere  | El ID de máquina virtual de la máquina virtual (es decir, “vm-12345”). |
| vmUuid | Todas                           | Código del conector de vSphere  | El UUID de la máquina virtual.                                         |

**Suplantación de usuario** El agente de App Layering, que se ejecuta como un servicio en un equipo Windows, se ejecuta en la cuenta del sistema local o en la cuenta de red. Cualquiera de estas cuentas puede tener algunos privilegios especiales, pero a menudo están restringidos cuando se ejecutan comandos específicos o se ven archivos en el sistema de archivos. Por lo tanto, App Layering te da la opción de agregar un usuario de dominio y una contraseña que se pueden usar para “suplantar” a un usuario. El script se puede ejecutar como si ese usuario hubiera iniciado sesión en el sistema, de modo que se pueda acceder a todos los comandos o datos con esos derechos y permisos de usuario. Si no se especifica ningún nombre de usuario o contraseña, el script se ejecuta mediante la cuenta en la que está configurado para ejecutarse el servicio.

**Directiva de ejecución de scripts** Los requisitos de la directiva de ejecución de scripts dependen de usted. Si tiene intención de ejecutar scripts sin firmar, debe configurar la directiva de ejecución en una de las directivas más indulgentes. Sin embargo, si firma sus propios scripts, puede optar por utilizar una directiva de ejecución más restrictiva.

### Mensajes de error

Si recibe errores ENOTFOUND al implementar una máquina de empaquetado o publicar una imagen, utilice la dirección IP en lugar del FQDN del servidor de vCenter.

## Recursos compartidos de archivos de red

May 9, 2024

Cuando se instala el dispositivo de App Layering, se configura un recurso compartido de archivos de red para utilizarlo como configuración de conector al crear capas y publicar imágenes por capas. Esta configuración del conector contiene las credenciales y la ubicación del recurso compartido de

archivos de red del dispositivo para que pueda implementar una máquina de empaquetado en el recurso compartido de archivos al crear capas o publicar imágenes por capas.

Cada configuración de conector se configura para acceder a una ubicación de almacenamiento mediante una cuenta específica. Para obtener más información sobre los conectores y las configuraciones de conectores, consulte [Conectar](#).

## Ubicación compartida de archivos de red

El nombre de la configuración del conector de recurso compartido de archivos de red incluye su ubicación. Busque la carpeta en el nivel superior del recurso compartido de archivos de red. Para obtener más información, consulte [Configurar un recurso compartido de archivos](#).

## Cuándo seleccionar el recurso compartido de archivos de red como configuración de conector

Cuando publique imágenes en capas en un servicio de Provisioning Services para el que aún no disponemos de un conector, puede seleccionar la **configuración del conector de recursos compartidos de archivos de red**. A continuación, puede copiar la imagen en capas desde el recurso compartido de archivos de red a la ubicación correcta para los servidores de Provisioning.

## Uso compartido de archivos de Windows

May 9, 2024

Una configuración de recursos compartidos de archivos de Windows contiene las credenciales y la ubicación de almacenamiento que el dispositivo necesita para conectarse a un recurso compartido de archivos. Utilice la **configuración del conector para compartir archivos de Windows** para publicar imágenes en capas.

Para obtener más información sobre los conectores y las configuraciones de conectores, consulte [Conectar](#).

## Antes de comenzar

Asegúrese de tener las siguientes configuraciones:

- Una configuración de conectores con Composición de descarga habilitada que admite capas de empaquetado.

- Un recurso compartido de archivos de red al que se puede acceder a través de SMB desde las máquinas de empaquetado creadas por el conector de empaquetado.

### Si esta es la primera vez que usa App Layering

Si es la primera vez que usa App Layering y quiere publicar discos de imágenes en capas en un recurso compartido de archivos de red, puede crear una configuración de conectores para cada una de sus ubicaciones de publicación.

Al publicar una imagen en capas, puede seleccionar una configuración de conector. Si aún no tiene la configuración de conectores correcta para la tarea, puede crear una haciendo clic en **Agregar configuración de conectores** en la página **Conectores**.

### Información necesaria para los ajustes de configuración de Windows File Share Connector

En la **consola de administración**, seleccione **Conector > Agregar configuración de conector > Uso compartido de archivos de Windows** y haga clic en **Nuevo**.

Para configurar el recurso compartido de archivos de Windows, especifique los valores siguientes:

- **Nombre de configuración:** nombre útil para ayudar a identificar y rastrear la configuración de este conector.
- **Ruta de uso compartido de archivos SMB:** ruta de uso compartido de red en la que se deben publicar los discos de imágenes en capas.
- **Nombre de usuario:** nombre de un usuario con permisos de lectura y escritura en la ruta de uso compartido especificada.
- **Contraseña:** contraseña del usuario indicado.

### Configuración de composición

- **Configuración del conector de descarga:** una configuración de conector de hipervisor con la composición de descarga habilitada. Esta configuración de conector compone la capa en nombre del conector de **recurso compartido de archivos de Windows**. La configuración de la máquina virtual que utiliza el motor de composición de descarga proviene de esta configuración de conector. Por ejemplo, si la configuración del conector de descarga está configurada para crear máquinas UEFI, la imagen resultante está en formato UEFI.
- **Formato de disco:** formato de disco virtual para publicar imágenes como en el recurso compartido de archivos de red. Puede ser VHD o VHDX.

## Capa

May 9, 2024

Una capa es un disco virtual que contiene el software del sistema operativo, las herramientas de plataforma, las aplicaciones o los datos y la configuración del usuario.

Al crear una capa, el dispositivo guarda la nueva capa como disco vDisk en el entorno del hipervisor y conecta el disco a una máquina de empaquetado.

Una vez creada, cada capa se almacena en un repositorio como disco vDisk.

### Tipos de capas

Puede utilizar los siguientes tipos de capas:

- Capas que crea en el hipervisor e incluye en las plantillas de imágenes que usa para publicar imágenes en capas.
- Capas que habilita en las plantillas de imagen y, por tanto, en las imágenes por capas que publique.

### Capas que se incluirán en plantillas de imagen e imágenes en capas

Puede crear capas para su sistema operativo, sus herramientas de plataforma y las aplicaciones que quiere entregar a los usuarios.

- **Capa de sistema operativo:** la capa en la que se instala el sistema operativo Windows desde la imagen ISO. Puede reutilizar la misma capa del sistema operativo con todas las capas de plataforma y aplicación compatibles. Recomendamos crear solo una capa del sistema operativo para cada versión principal de Windows, por ejemplo, una para Windows 10 y otra para Windows Server 2016. Puede agregar nuevas versiones de una capa para cada versión de continuación. Por ejemplo, si tiene una capa de Windows 10, versión 1709, le agregará una versión para la versión 1809 y otra para 1903. Cuando actualice la capa del sistema operativo, no es necesario actualizar las capas de la aplicación, pero *actualice* la capa de la plataforma. Para obtener más información sobre la creación de una capa de sistema operativo, consulte [Crear la capa de SO](#).
- **Capas de plataforma:** capa en la que se instala y configura el software para un entorno local o en la nube específico. Al aislar el software de infraestructura en una capa de plataforma, puede reutilizar la misma capa de SO y capas de aplicación en varios hipervisores. Puede crear una capa de plataforma para cada parte de la infraestructura si, por ejemplo, utiliza más de un Hipervisor.

Si utiliza cualquiera de los siguientes software en su infraestructura, normalmente los instala en una capa de plataforma:

- Software de agente de conexión
- Software de aprovisionamiento
- System Center Configuration Manager (SCCM)

Aunque no parezca intuitivo, es fundamental instalar el software en el primer *hipervisor* que admita en la *capa del sistema operativo*.

Si admite más de un Hypervisor, puede crear otra capa de plataforma para el hipervisor adicional. La capa de plataforma para un Hypervisor adicional debe incluir el software del hipervisor, junto con el software de Provisioning, el broker de conexiones y el software SCCM. Cuando cree esta capa de plataforma adicional, asegúrese de activar la casilla de verificación del nuevo hipervisor que admite. Esto garantiza que el dispositivo de App Layering elimine los archivos y la configuración originales del hipervisor de la capa del sistema operativo para que no interfieran con el rendimiento.

Para obtener más información sobre la creación de una capa de SO, consulte [Crear capa de plataforma](#).

- **Capas de aplicaciones:** las capas en las que se instalan las aplicaciones. Normalmente, recomendamos instalar una aplicación en cada capa, aunque puede incluir más. Para facilitar el mantenimiento, incluya aplicaciones que estén en el mismo programa de actualización. Si una aplicación requiere otras aplicaciones, cree primero la capa para la aplicación requerida. Para obtener más información sobre la creación de una capa de aplicaciones, consulte [Crear o clonar una capa de aplicaciones](#). Para obtener consejos sobre la superposición de una aplicación específica, consulte [Recetas de App Layering](#).

### Capas que puede habilitar en imágenes en capas

Además de las capas que se incluyen en las imágenes en capas, puede habilitar las capas elásticas y User en ellas mediante la configuración de la plantilla de imagen:

- **Capas elásticas:** capas de aplicaciones que se asignan a usuarios específicos y se entregan cuando los usuarios inician sesión. Una capa de aplicación elástica no está incluida en la imagen base, pero se entrega en ella. Las aplicaciones elásticas aparecen en el escritorio del usuario.

#### Importante:

Una capa de aplicación se puede entregar a un usuario como parte de la imagen en capas o como una capa elástica.

Hay algunas aplicaciones que no se pueden usar como capas elásticas, por ejemplo, Microsoft Office. Para saber si una aplicación tiene esta limitación, consulte las recetas de App Layering



[aquí](#) y el [foro de capas de aplicaciones](#) para obtener notas sobre cómo crear capas de una aplicación. Si no se especifican limitaciones para su aplicación, puede asignarla como una capa elástica. Para obtener más información sobre cómo habilitar y asignar capas elásticas en una imagen en capas, consulte [Implementar capas de aplicaciones como capas elásticas](#).

- **Capas de usuarios:** al habilitar las capas de usuarios en una imagen en capas, puede conservar los datos y la configuración de un usuario, así como cualquier aplicación que instale él mismo. Cuando se habilita, se crea una capa de usuarios para cada usuario la primera vez que inicia sesión en una imagen. Para habilitar esta función, seleccione la configuración **de capas de usuario** en la plantilla de imagen que utiliza para publicar la imagen en capas. Para obtener más información sobre cómo habilitar capas elásticas en una imagen en capas, consulte [Implementar capas de usuarios](#) y [Crear o clonar una plantilla de imagen](#).

No asigne capas de aplicaciones que tengan exploradores como Chrome o Firefox a los usuarios cuando esos usuarios inicien sesión en una imagen que utilice capas de usuario completas. Los exploradores se actualizan con frecuencia, lo que puede provocar conflictos de revisión entre la capa grabable del usuario y la revisión de la imagen de arranque. Sin embargo, puede asignar esas capas a los usuarios si están iniciando sesión en una imagen que sea el host de una sesión.

### Aplicaciones que requieren un usuario o administrador local

La capa del sistema operativo conserva los usuarios o grupos locales que agregue, pero las capas de aplicaciones, las capas de plataforma y las capas de usuarios no lo hacen. Por ejemplo, los usuarios y grupos que agrega o cambia al instalar una aplicación en una capa de aplicación, capa de plataforma o capa de usuarios no persisten. Puede:

- Agregue el usuario local o el administrador a la capa del sistema operativo antes de instalar la aplicación.
- Instale la aplicación en la capa del sistema operativo.

### Introducción a la integridad de capa

Al crear una capa de SO, aplicación o plataforma, comienza la creación de capas en la consola de administración de App Layering y, a continuación, instala el software en la máquina virtual especificada en el hipervisor. Cuando la capa está en el estado en el que quiere que esté cuando los usuarios inicien sus escritorios, apague el equipo y finalice la capa.

Cuando cierra una capa para finalizarla, las operaciones `Ngen.exe` de Windows muestran mensajes sobre las tareas pendientes que deben completarse antes de cerrarse. Debe dejar que estos trabajos se completen, pero puede acelerar las operaciones `Ngen.exe`, si es necesario. Los detalles sobre los mensajes `Ngen.exe` y cómo acelerar las operaciones se incluyen en cada uno de los artículos de capas relacionados:

- Preparar la imagen del sistema operativo para la disposición en capas en XenServer, Hyper-V o vSphere
- Preparar la imagen del sistema operativo para la disposición en capas en Azure
- Preparar la imagen del sistema operativo para la disposición en capas en Nutanix
- Crear capa de plataforma
- Crear o clonar una capa de aplicación
- Actualizar capa
- Solucionar problemas de integridad de capa

### **Prioridad de capa**

La prioridad de capa define el orden de capa al crear el sistema de archivos de Windows y el Registro. La prioridad de capa es importante cuando:

- Composición de capas como parte de la publicación de imágenes en capas.
- Búsqueda de capas para la configuración del archivo y del Registro.
- Proporcionar capas elásticas y capas de usuarios a los escritorios de los usuarios.

El software App Layering asigna una prioridad a cada capa y aplica las capas en orden, desde la prioridad más baja hasta la más alta.

En Windows, la capa de prioridad más alta tiene prioridad. Si existe un archivo o una entrada del Registro en dos capas, Windows utiliza el archivo o la entrada del Registro de la capa con la prioridad más alta.

### **Cómo se determina la prioridad de capa**

La prioridad de una capa se basa en el tipo de capa y, para las capas de aplicación, en el orden en que se crearon las capas.

**Capas dentro de la imagen base** Las capas que forman parte de la imagen en capas se aplican en orden, con la capa de plataforma siempre aplicada en último lugar, como la capa de prioridad más alta.

Como se muestra en la tabla siguiente, la prioridad asignada a las capas de la aplicación se basa en el orden en el que se crean las capas. Las capas de aplicaciones más recientes tienen una prioridad más alta que las capas más antiguas.

| Prioridad | Tipo de capa                                       |
|-----------|----------------------------------------------------|
| Alto      | Capa de plataforma                                 |
|           | Capa de aplicaciones creada por última vez         |
| Medio     | Capas de aplicación en orden por fecha de creación |
|           | La capa de aplicaciones creada primero             |
| Bajo      | Capa de sistema operativo                          |

Si las capas tienen un archivo o una entrada del Registro en común, se utiliza el archivo o la entrada del Registro de las capas de prioridad superior.

**Capas habilitadas en la imagen base** Cuando se inicia una imagen publicada, se pueden aplicar más capas, si las capas están habilitadas en la plantilla de imagen para la imagen en capas:

- Capas elásticas (capas de aplicaciones asignadas a los usuarios como capas elásticas)
- Capas de usuarios

Al fusionar capas en una imagen, las capas de usuarios son siempre la prioridad más alta. Las capas elásticas son las siguientes, y las capas de la imagen base duran.

Como se muestra en la tabla siguiente, la prioridad de las capas elásticas es la misma que la prioridad de las capas de aplicación originales, pero se aplica a la imagen base. La prioridad de la capa elástica *no* depende del orden en que las capas se enlazan a la imagen publicada.

| Prioridad | Tipo de capa                                                |
|-----------|-------------------------------------------------------------|
| Alto      | Capa de usuarios                                            |
|           | Capa elástica: Capa de aplicaciones creada por última vez   |
| Medio     | Capas elásticas: Capas de aplicaciones en orden de creación |
|           | Elastic App: Capa de aplicaciones creada primero            |
| Bajo      | Imagen en capas: Todas las capas dentro de la imagen base   |

## Conflictos de prioridad de

La mayoría de las capas de aplicaciones funcionan, pero en algunas situaciones, el orden en el que se instalan las aplicaciones puede provocar conflictos en el escritorio.

Si una aplicación debe instalarse antes que otra, cree las capas en el orden requerido. El software App Layering aplica las capas en el mismo orden.

Si dos capas entran en conflicto y sospecha que se debe al orden en que se incorporan a la imagen, tiene dos opciones:

- Vuelva a crear la capa que quiere instalar en último lugar, de modo que se incorpore en el orden correcto.
- Solicite ayuda a la Asistencia técnica.

## Preparar el sistema operativo para la distribución por capas

May 9, 2024

Puede preparar su sistema operativo para la colocación en capas en cualquier momento, incluso si aún no se ha instalado el software de App Layering. Es importante que cumpla con todos los requisitos para que la capa del sistema operativo funcione correctamente en su entorno.

Una vez que haya cumplido los requisitos y se haya familiarizado con las directrices sobre qué incluir en la capa de SO, utilice las instrucciones para preparar el sistema operativo en el entorno del hipervisor. Si posteriormente amplía la compatibilidad con otro hipervisor, puede volver a utilizar esta capa de SO instalando las herramientas para el segundo hipervisor en la capa Plataforma que cree para ese segundo entorno.

## Requisitos y recomendaciones

Al preparar una imagen del sistema operativo, cumpla con los siguientes requisitos y tenga en cuenta las recomendaciones relacionadas.

- **Una capa de sistema operativo para cada versión de Windows que administre (recomendado):** Citrix recomienda preparar una única imagen del sistema operativo para cada versión de Windows que administre, junto con un conjunto de capas de plataforma y aplicación para cada una.
- **Imagen nueva del sistema operativo:** comience con una imagen nueva de un [sistema operativo Windows compatible](#) del hipervisor. Esto garantiza que la imagen esté optimizada para su entorno.

- **Dirección IP de DHCP:** asegúrese de que la imagen del sistema operativo *no* esté en un dominio. Asegúrese de que la imagen obtiene su dirección IP de DHCP. De lo contrario, no puede instalar App Layering OS Machine Tools. La unión de dominios se puede hacer en la capa de plataforma.
- **Machine Tools del SO de App Layering:** busque las Machine Tools del sistema operativo en el paquete de instalación de App Layering.
- **Script de optimización para MS Office:** si va a ejecutar MS Office, debe usar el script de optimización incluido en el paquete de instalación.

### XenServer, MS Hyper-V o VMware vSphere

En el raro caso de que necesite ejecutar el programa de instalación de Windows Mini, puede modificar el archivo.hta unattend.hta que proporcionamos para sus necesidades.

- **Archivo de respuesta para la instalación desatendida (opcional):** el archivo de respuesta se incluye en la descarga de App Layering.

#### Notas:

Evite utilizar scripts de terceros, ya que pueden cambiar los servicios y funciones que utiliza el servicio de App Layering, por ejemplo, Universal Plug and Play y la configuración de nombres de archivo 8.3.

### Qué incluir en la capa de SO

Incluya el software y la configuración siguientes en la capa de SO:

- **Herramientas de hipervisor:** debe incluir las herramientas de hipervisor en la capa de sistema operativo. Puede actualizar las herramientas agregando una nueva versión a la capa.

#### Notas:

- Cuando actualice las herramientas del hipervisor en la capa de SO, pruebe la capa de plataforma existente para ver si necesita actualizarse. Según la plataforma y qué otras cosas estén instaladas en ella, es posible que tenga que volver a crear la capa de plataforma.
- Si utiliza la misma capa de sistema operativo con varios hipervisores, tiene sentido instalar las herramientas del hipervisor en capas de plataforma especialmente diseñadas para esos hipervisores.

- **.NET Framework v4.0 o posterior:** Incluya .NET Framework v4.0 o posterior para que las actualizaciones de Windows solo sean necesarias en la capa del sistema operativo. Por ejemplo, se requiere .NET 4.8 para que Citrix Virtual Apps and Desktops (CVAD) 2303 agregue un VDA.

- **.NET Framework 3.5 (al crear una capa de MS Office):** Para facilitar la actualización, instale todas las versiones de .NET Framework en la capa de sistema operativo *antes* de crear la capa de Office. Si .NET Framework v3.5 no está presente al instalar Office, Office lo instala por usted y no se recomienda tener versiones o actualizaciones de .NET Framework instaladas en capas de aplicación.
- **Deshabilitar las actualizaciones de Windows mediante el GPO local:** deshabilite las actualizaciones de Windows en la capa de sistema operativo y hágalo con el GPO local en lugar del Servicio de actualización de Windows.
- **Eliminación de aplicaciones de la Tienda Windows:** si eliminas aplicaciones de la Tienda Windows, quítalas de la capa de sistema operativo, no de una capa de aplicaciones.
- **Activación de Windows:** utilice KMS para la activación de Windows. Al crear la capa de sistema operativo, ejecute **SetKMSVersion.exe** para configurar los scripts de inicio que activan la versión correcta de Windows.
- **Cuentas de usuario y grupos:** cualquier cuenta de usuario o grupo adicional debe crearse en la capa de sistema operativo. Cualquier cambio de pertenencia a grupos de dominio debe realizarse a través de la Directiva de grupo.
- **Aplicaciones que crean usuarios locales:** incluye aplicaciones que creen usuarios locales para garantizar que se capturan los cambios en los grupos locales y los usuarios locales, algo que no se hace en las capas Plataforma y Aplicación.

### Qué *no* incluir en la capa de sistema operativo

No incluya el siguiente software en la capa de SO.

- **Software de aprovisionamiento:** el software asociado a su servicio de aprovisionamiento debe estar instalado en la capa de plataforma, no en la capa de sistema operativo.
- **Software de agente de conexiones:** el software de agente de conexión también debe estar instalado en la capa de plataforma, no en la capa de sistema operativo.
- **MS Office y otras aplicaciones:** *no* incluya MS Office ni otras aplicaciones en la capa del sistema operativo, excepto las pocas aplicaciones que crean usuarios locales. Generalmente, las aplicaciones deben instalarse en capas de aplicaciones.
- **Unión a un dominio:** *no* una la capa de SO a un dominio de Active Directory. En su lugar, únete al dominio en la capa Plataforma. Esto le permite usar el mismo sistema operativo en diferentes dominios.
- **Indicador de depuración: el indicador** de depuración no se puede habilitar en ninguna entrada de arranque BCD de la capa de sistema operativo si se utiliza el arranque seguro. No importa si el indicador es verdadero o falso; el indicador en sí no puede estar presente, ya que se sabe que causa problemas.

Para obtener pasos detallados para preparar el sistema operativo, seleccione su hipervisor:

- [XenServer, Hyper-V, vSphere](#)
- [Azure](#)
- [Nutanix](#)

## Preparar la imagen del sistema operativo para la disposición en capas en XenServer, Hyper-V o vSphere

May 9, 2024

Antes de empezar, asegúrese de que cumple los [requisitos](#). Mientras prepara la imagen, puede [acelerar una operación de Microsoft Ngen.exe, si es necesario](#), si cree que está tardando demasiado.

Si utiliza Windows 10, puede acelerar los tiempos de inicio de los escritorios siempre y cuando *no* esté ejecutando Citrix Provisioning, creación de máquinas o VMware View. En esta situación, puede [eliminar las aplicaciones integradas de Windows 10](#). Recomendamos eliminar las aplicaciones en una *nueva versión* de la capa del sistema operativo, en lugar de hacerlo en la propia imagen del sistema operativo.

### Nota:

XenServer admite máquinas basadas en UEFI después de agregar un nuevo conector de XenServer.

## Instalar el SO en una máquina virtual

Es fundamental comenzar con un sistema operativo recién instalado desde ISO, preferiblemente desde su hipervisor.

En este procedimiento, asegúrese de seguir los pasos y notas específicos de la versión de Windows que está instalando.

1. Inicie sesión en su cliente de hipervisor.
2. Cree una máquina virtual con la configuración correcta de CPU, RAM, disco duro y red para su tipo de sistema operativo. Orientación:
  - **Máquina virtual de XenServer:** Asegúrese de seleccionar solo una red.
  - **Máquina virtual vSphere:**
    - **Red:** (Necesario) Seleccione el **adaptador de red VMXNET 3**.

**Importante:**

Puede tener un solo dispositivo de red, y *nunca se debe haber utilizado* la NIC E1000. El adaptador E1000 predeterminado (o incluso una NIC fantasma sobrante de un adaptador E1000) puede causar errores de tiempo de espera de personalización en las máquinas virtuales.

- **Aprovisionamiento ligero:** seleccione **Thin Provision**.

- **Todos los hipervisores:**

- **Disco duro:** asegúrese de que el dispositivo pueda acceder al disco duro que cree.
3. Conecte la ISO e instale el sistema operativo. **Esta máquina no debe estar unida al dominio.** La unión a un dominio debe realizarse en la capa de plataforma y cualquier cambio de pertenencia a un grupo de dominios debe realizarse mediante la directiva de grupo.
  4. Instale las herramientas de hipervisor de la plataforma en la que planea empaquetar capas. Si admite varios hipervisores, coloque las herramientas para el hipervisor que planea usar para publicar imágenes en la capa Plataforma.
    - **Para Hyper-V:** Utilice el disco de configuración de Microsoft Windows Integration Services para instalar Hyper-V Integration Services.

### **Si utiliza un SO de servidor, instale la función Host de sesión de Escritorio remoto**

Al utilizar un servidor Windows Server, debe instalar la función **Host de sesión de Escritorio remoto**. Cuando la función **Host de sesión de Escritorio remoto** está instalada en la capa del sistema operativo, se actualiza como parte de Windows. Si lo prefiere, puede instalar el rol en la capa de plataforma con el VDA.

Si instala RDS en la capa de SO, debe utilizar GPO locales para definir los servidores de licencias de RDS. De lo contrario, con el tiempo perderá la capacidad de iniciar sesión en máquinas de empaquetado.

Para instalar la función Host de sesión:

1. En el **Administrador del servidor**, seleccione **Agregar funciones y características**.
2. En **Tipo de instalación**, seleccione la instalación **Por roles** o **Por funciones**.
3. Para la función **Servidor**, seleccione **Servicios de Escritorio remoto > Host de sesión de Escritorio remoto (instalado)**. Esto instala la biblioteca de C++ y el rol de RDS.
4. Complete el proceso de agregar los roles de servidor.



## Asegúrese de que estén instaladas las versiones correctas de .NET Framework (Windows 10 y Windows Server 2016)

.NET Framework es un marco de software proporcionado por Microsoft y es necesario para que se ejecuten muchas aplicaciones de terceros. Cualquier instalación de .NET Framework debe incluirse en la capa del sistema operativo. Esto incluye .NET 3.5 y .NET 4.0 o versiones posteriores.

### Nota:

Citrix Virtual Apps and Desktops (CVAD) 2303 requiere la versión 4.8 de .NET para agregar VDA.

Asegúrese de instalar .NET Framework y cualquier actualización en su capa de sistema operativo.

## Instalar actualizaciones de Windows

Asegúrese de instalar todas las actualizaciones de Windows.

1. Instale todas las actualizaciones importantes.
2. Compruebe si hay actualizaciones de nuevo después de reiniciar la máquina virtual. Algunas actualizaciones solo están disponibles después de instalar otras.
3. Instale todos los Service Packs necesarios:
  - Si usa Windows 2008 con Citrix Provisioning, instale Windows Server 2008 R2 Service Pack 1 (SP1).

### Nota:

Si está instalado KB3125574, desinstálelo antes de instalar este service pack.

4. Desactive **las actualizaciones automáticas de Windows** e inhabilite la **restauración del sistema** de Windows mediante el editor de directivas de grupo local, `gpedit.msc`. El sistema gestiona los puntos de restauración por usted. Las versiones de capa permiten especificar cuándo se producen actualizaciones.
5. **Windows 10:** Borre la hibernación mediante este comando:

```
1 powercfg.exe /hibernate off
2 <!--NeedCopy-->
```

6. Active el administrador integrado y seleccione **La contraseña nunca caduca**.
7. Si utiliza licencias del Servicio de administración de claves (KMS), ejecute una ventana de comandos como Administrador e introduzca los siguientes comandos:

```
1 slmgr /skms <kmsserverhost>
2 slmgr /rearm
3 reboot
4 slmgr /ipk XXXX-YOUR-KMS-KEY-XXXX
5 slmgr /ato
6 <!--NeedCopy-->
```

8. Si utiliza un sistema operativo de servidor, ejecute los siguientes comandos en PowerShell:

```
1 Set-ExecutionPolicy Unrestricted
2 Enable-PSRemoting
3 <!--NeedCopy-->
```

### Acelere una operación de Microsoft Ngen.exe, si es necesario

Una vez instaladas todas las actualizaciones de software, debe permitir a `Ngen.exe` básicamente recompilar código de bytes `.NET` en imágenes nativas y construir las entradas del registro para administrarlas.

`Ngen.exe` es el generador de imágenes nativas de Microsoft, que forma parte del sistema `.NET`. Windows determina cuándo se ejecuta `Ngen.exe` en función del software que se está instalando y de lo que detecta Windows en la configuración.

#### Importante:

Cuando `Ngen.exe` se esté ejecutando, debe dejar que se complete. Una operación `Ngen.exe` interrumpida puede ocasionar que los ensamblados `.NET` no funcionen o que haya otros problemas en el sistema `.NET`.

Normalmente, `Ngen.exe` es una operación en segundo plano que se detiene cuando hay una actividad en primer plano. Si quieres acelerar una operación `Ngen.exe`, puede poner la tarea en primer plano para completarla lo antes posible.

Para poner la tarea en primer plano:

1. Abra un símbolo del sistema como Administrador.
2. Vaya al directorio `Microsoft.NET\Framework` de la versión actualmente en uso:

```
1 cd C:\Windows\Microsoft.NET\FrameworkNN\vX.X.XXXXX
2 <!--NeedCopy-->
```

3. Introduzca el siguiente comando `Ngen.exe` para ejecutar todos los elementos en cola. Este comando procesa las instalaciones de componentes en cola antes de crear ensamblajes.

```
1 ngen eqi 3
2 <!--NeedCopy-->
```

**Nota:**

Esta variación del `ngen` comando se ha probado y es la variante que funciona en esta situación en App Layering.

La tarea `Ngen.exe` pasa al primer plano de la línea de comandos y muestra una lista de los ensamblados que se están compilando. Está bien si ve mensajes de compilación.

Puede utilizar el **Administrador de tareas** para ver si `MSCORSVW.EXE` se está ejecutando una instancia de. Si es así, permite que se complete o se ejecute `ngen eqi 3`.

**Advertencia:**

No reinicie para detener la tarea. ¡Permita que la tarea se complete!

4. Asegúrese de que todos los procesos `Ngen.exe` se han ejecutado hasta su finalización.

### Ejecute las Machine Tools del sistema operativo de App Layering en la imagen

Para preparar la imagen del sistema operativo para que se ejecute en una capa, ejecute el archivo de herramientas de máquinas del sistema operativo en la imagen. Este ejecutable ejecuta un script de instalación de GPO (`gposetup.cmd`) y un script para establecer la versión del Servicio de administración de claves (KMS). El script se llama `SetKMSVersion.hta`.

1. Descargue el siguiente archivo zip en la imagen del sistema operativo:  
`App_Layering_Citrix_App_Layering_OS_Machine_Tools_20.x.zip`
2. Extraiga los archivos a:

```
1 c:\windows\setup\scripts
2 <!--NeedCopy-->
```

**Nota:**

El archivo debe extraerse al directorio. No cambie el directorio.

### Si utiliza KMS, configure la activación de la licencia

Una vez extraídos los scripts del Servicio de administración de claves (KMS), la utilidad `SetKMSVersion` le pide que elija si quiere utilizar licencias de KMS.

**Nota:**

La publicación de imágenes en entornos en los que se utilizan simultáneamente la activación basada en KMS y Active Directory (ADBA) provoca problemas de activación.

1. En el cuadro de diálogo que aparece, seleccione si quiere utilizar las licencias del Servicio de administración de claves (KMS).



Para configurar scripts para KMS, haga lo siguiente.

1. Ir a:  
`c:\windows\setup\scripts`
2. Ejecute **SetKMSVersion.hta** como administrador para crear un script en el archivo `c:\windows\setup\scripts\kmsdir` folder.

Cuando se inicia el sistema operativo, se ejecuta el script de activación de KMS apropiado.

## Instalar los servicios App Layering

1. En la carpeta `c:\windows\setup\scripts`, ejecute **setup\_x86.exe (32 bits)** o **setup\_x64.exe (64 bits)**.

Está listo para [importar la imagen](#) en una nueva capa del sistema operativo.

### Nota:

Asegúrese de que el instalador de las herramientas de preparación de imágenes se ejecute una vez antes de importar el sistema operativo. No ejecute el instalador de las herramientas de preparación de imágenes después de importar el sistema operativo, ya que esto podría provocar problemas desconocidos.

## Preparar la imagen del sistema operativo para la colocación en capas en Google Cloud

January 19, 2022

En este tema se explica cómo preparar una imagen limpia del sistema operativo para importarla en una nueva capa de SO. Antes de empezar, asegúrese de cumplir con los [requisitos](#). Mientras preparas la imagen, puedes hacerlo [Agilizar las operaciones de Microsoft Ngen.exe](#), si crees que está tardando demasiado.

Si utiliza Windows 10 y *no* ejecuta Citrix Provisioning, creación de máquinas Citrix o View, puede acelerar los tiempos de inicio del escritorio [quite las aplicaciones integradas de Windows 10](#). Sin embargo, recomendamos eliminar las aplicaciones en una *nueva versión* de la capa de sistema operativo, *no* en la propia imagen del sistema operativo.

### Instalar el SO en una máquina virtual

1. Familiarícese con las pautas para [preparación de una capa de SO](#), incluidos los requisitos y las recomendaciones. Asegúrese de leer las secciones sobre qué incluir y qué no incluir en una capa de sistema operativo.
2. Navegue hasta el [Portal de Google Cloud](#).
3. Selecciona **Marketplace** en la columna de la izquierda e implementa una nueva máquina virtual.

#### Nota:

Al configurar la nueva red de instancias, asegúrese de que la máquina virtual esté en una red a la que pueda acceder el dispositivo.

4. Si utiliza un sistema operativo Windows Server, desplácese hasta **Sistemas operativos** y seleccione un sistema operativo **Windows Server 2019** o **Windows Server 2016**.
5. Si va a traer Windows 10 desde otra plataforma (no está disponible en el Marketplace), siga los pasos que se indican en [Tutorial sobre cómo traer sus propias licencias](#).
6. Configure la nueva instancia:
  - Al seleccionar una red para la nueva instancia, asegúrese de que la máquina virtual esté en una red a la que pueda acceder el dispositivo.
  - Al seleccionar el almacenamiento, cualquier tipo de almacenamiento está bien.

## Ejecute las Machine Tools del sistema operativo de App Layering en la imagen

1. En el nuevo equipo, abra un navegador web, navegue hasta el Centro de descargas y descargue las **máquinas herramientas del sistema operativo**.
2. Descargue el siguiente archivo zip en la imagen del sistema operativo:

```
1 Citrix_App_Layering_OS_Machine_Tools_20.x.x.exe
2 <!--NeedCopy-->
```

3. Ejecute el archivo y copia los archivos en:

```
1 c:\windows\setup\scripts
2 <!--NeedCopy-->
```

**Nota:**

El archivo debe extraerse en el directorio anterior. No cambie el directorio.

## Si utiliza el Servicio de administración de claves, configure la activación de licencias

Una vez extraídos los scripts, la `SetKMSVersion` utilidad le pide que elija si desea utilizar las licencias del Servicio de administración de claves (KMS).

**Nota:**

La publicación de imágenes en entornos en los que se utilizan la activación basada en KMS y Active Directory (ADBA) al mismo tiempo causa problemas con la activación.

1. En el cuadro de diálogo siguiente, seleccione si quiere utilizar las licencias del Servicio de administración de claves (KMS).



Para configurar scripts para KMS, haga lo siguiente.

1. Desplácese hasta:

```
1 c:\windows\setup\scripts
2 <!--NeedCopy-->
```

2. Ejecute **SetKMSVersion.exe** como administrador para crear un archivo de script en la `c:\windows\setup\scripts\kmsdir` carpeta.

Cuando se inicia el sistema operativo, se ejecuta el script de activación de KMS apropiado.

### Instalar los servicios App Layering

1. En la nueva máquina, desplácese hasta `C:\Windows\Setup\scripts` y ejecute **setup\_x64.exe** para instalar los controladores de App Layering en la máquina del sistema operativo.
2. La instalación le solicita la ubicación del archivo Unattend.xml (la ubicación predeterminada es `C:\windows\panther`).
3. Asegúrese de que esta máquina no está unida a un dominio.
4. Realice reinicios pendientes en la máquina del sistema operativo para que pueda importar esta imagen en una capa.
5. Asegúrese de que la nueva máquina del sistema operativo esté en uno de los siguientes estados antes de continuar.
  - Running
  - Detenido
  - Detenido (desasignado)

### Acelere una operación de Microsoft Ngen.exe, si es necesario

Una vez que se hayan instalado todas las actualizaciones de software, debe `Ngen.exe` permitir, esencialmente, volver a compilar código de `.NET` bytes en imágenes nativas y construir las entradas del registro para administrarlas.

`Ngen.exe` es Microsoft Native Image Generator, que forma parte del `.NET` sistema. Windows determina cuándo se debe ejecutar en `Ngen.exe` función del software que se está instalando y qué detecta Windows en la configuración.

#### Importante:

Cuando `Ngen.exe` se está ejecutando, debes dejar que se complete. Una `Ngen.exe` operación interrumpida puede dejarle con `.NET` ensamblajes que no funcionan u otros problemas en el .

NET sistema.

Normalmente, `Ngen.exe` es una operación en segundo plano que se detiene cuando hay actividad en primer plano. Si desea acelerar una `Ngen.exe` operación, puede poner la tarea en primer plano para completarla lo antes posible.

Para poner la tarea en primer plano:

1. Abra un símbolo del sistema como Administrador.
2. Vaya al `Microsoft.NET\Framework` directorio de la versión que se está utilizando actualmente:

```
1 cd C:\Windows\Microsoft.NET\FrameworkNN\vX.X.XXXXX
2 <!--NeedCopy-->
```

3. Introduzca el siguiente `Ngen.exe` comando para ejecutar todos los elementos en cola. Este comando procesa las instalaciones de componentes en cola antes de crear ensamblajes.

```
1 ngen eqi 3
2 <!--NeedCopy-->
```

La `Ngen.exe` tarea se mueve al primer plano en el símbolo del sistema y enumera los ensamblajes que se están compilando. Está bien si ve mensajes de compilación.

Puede utilizar el **Administrador de tareas** para ver si `MSCORSVW.EXE` se está ejecutando una instancia de. Si lo es, permita que se complete o ejecute `ngen update eqi 3`.

### Precaución:

No reinicie para detener la tarea. ¡Permita que la tarea se complete!

4. Asegúrese de que todos los `Ngen.exe` procesos se hayan ejecutado hasta su finalización.

## Preparar la imagen del sistema operativo para la disposición en capas en Azure

September 5, 2022

En este tema se explica cómo preparar una imagen limpia del sistema operativo para importarla en una nueva capa de SO. Antes de empezar, debe cumplir con los [requisitos](#). Mientras prepara la imagen, puede [acelerar las operaciones de Microsoft Ngen.exe](#), si cree que está tardando demasiado.

Si usa Windows 10 y *no* ejecuta Citrix Provisioning, una creación de máquinas o Vista, puede acelerar los tiempos de inicio del escritorio [eliminando las aplicaciones integradas de Windows 10](#). Sin



embargo, recomendamos eliminar las aplicaciones en una *nueva versión* de la capa del sistema operativo, *no* en la propia imagen del sistema operativo.

**Nota:**

No utilice un archivo desatendido con un conector Azure de Machine Creation Services (MCS). El software App Layering elimina el archivo desatendido si está presente, porque no es necesario ni se recomienda para un conector de MCS Azure.

### Instalar el SO en una máquina virtual

1. En el [portal de Microsoft Azure](#), cree una nueva máquina virtual a partir de la imagen de Escritorio remoto de Windows Server seleccionando:

**Nuevo > Computar > Máquina virtual**

2. Complete el asistente Crear máquina virtual:

**Conceptos básicos:**

- **Nombre:** El nombre que especifique para la nueva máquina debe cumplir con las convenciones de nomenclatura de Azure.
- **Nombre de usuario y contraseña:** El nombre de usuario y la contraseña de la nueva máquina de servidor que especifique se utilizan para cualquier máquina de empaquetado que se cree que contenga esta capa de sistema operativo.
- **Ubicación del grupo de recursos:** Asegúrese de que el valor de la ubicación del grupo de recursos coincida con la ubicación de la cuenta de almacenamiento que configuró en la configuración del conector.

3. Seleccione la configuración de red necesaria.
4. Revise el resumen y cree la máquina virtual.
5. Inicie sesión en la nueva máquina virtual y reinicie la máquina.
6. Instale todas las actualizaciones importantes. Asegúrese de reiniciar el sistema y compruebe si hay más actualizaciones. Algunas actualizaciones solo están disponibles después de instalar otras.
7. Ejecute Windows Ngen.exe.
8. Quite o cambie el nombre del archivo Unattend en `C:\Windows\OEM`.
9. Para borrar las actualizaciones automáticas de Windows, seleccione:  
**Panel de control > Sistema y seguridad > Windows Update > Cambiar configuración**
10. Asegúrese de que esta máquina no está unida a un dominio.
11. Habilite el administrador integrado y compruebe que **la contraseña no caduca nunca**.

12. Si se trata de un SO de servidor, ejecute los siguientes comandos en PowerShell:

```
1 Set-ExecutionPolicy Unrestricted
2 Enable-PSRemoting
3 <!--NeedCopy-->
```

### Ejecute las Machine Tools del sistema operativo de App Layering en la imagen

1. En la nueva máquina, abra un explorador web, vaya al Centro de descargas y descargue OS Machine Tools.
2. Descargue el siguiente archivo zip en la imagen del sistema operativo:

```
1 Citrix_App_Layering_OS_Machine_Tools_20.x.x.exe
2 <!--NeedCopy-->
```

3. Ejecute el archivo y copia los archivos en:

```
c:\windows\setup\scripts
```

**Nota:**

El archivo debe extraerse en el directorio anterior. No cambie el directorio.

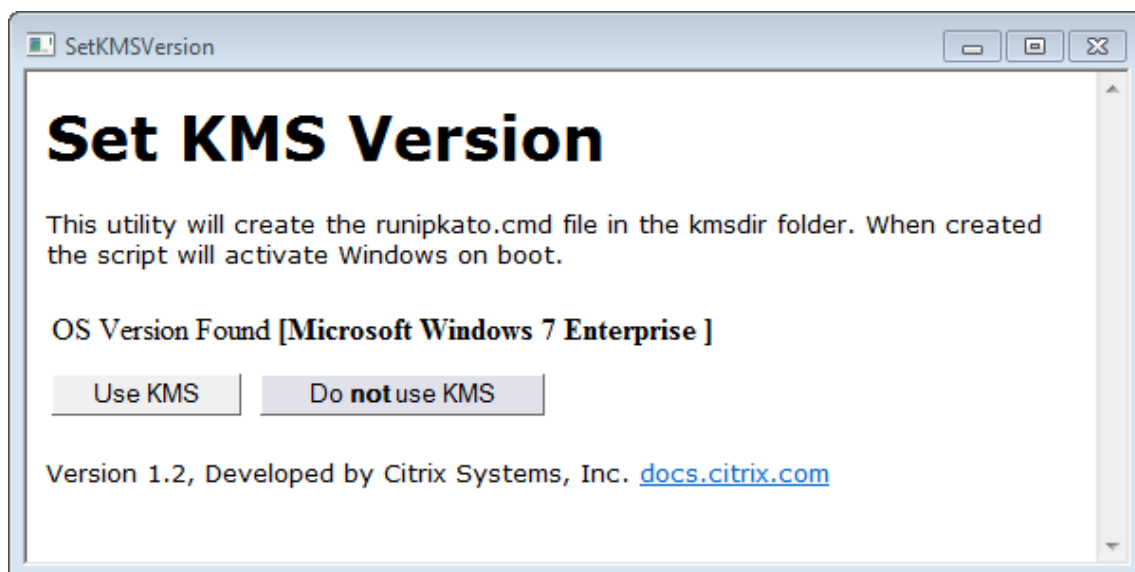
### Si utiliza el Servicio de administración de claves, configure la activación de licencias

Una vez extraídos los scripts, la utilidad `SetKMSVersion` le pide que elija si quiere utilizar las licencias del Servicio de administración de claves (KMS).

**Nota:**

La publicación de imágenes en entornos en los que se utilizan al mismo tiempo la activación basada en KMS y la activación basada en Active Directory (ADBA) provoca problemas de activación.

1. En el cuadro de diálogo siguiente, seleccione si quiere utilizar las licencias del Servicio de administración de claves (KMS).



Para configurar scripts para KMS, haga lo siguiente.

1. Desplácese hasta:

`c:\windows\setup\scripts`

2. Ejecute **SetKMSVersion.exe** como administrador para crear un archivo de script en la carpeta `c:\windows\setup\scripts\kmsdir`.

Cuando se inicia el sistema operativo, se ejecuta el script de activación de KMS apropiado.

### Instalar los servicios App Layering

1. En la nueva máquina, desplácese hasta `C:\Windows\Setup\scripts` y ejecute **setup\_x64.exe** para instalar los controladores de App Layering en la máquina del sistema operativo.
2. La instalación le solicita la ubicación del archivo Unattend.xml (la ubicación predeterminada es `C:\windows\panther`).
3. Asegúrese de que esta máquina no está unida a un dominio.
4. Realice reinicios pendientes en la máquina del sistema operativo para que pueda importar esta imagen en una capa.
5. Asegúrese de que la nueva máquina del sistema operativo esté en uno de los siguientes estados antes de continuar.
  - En ejecución
  - Detenido
  - Detenido (desasignado)

## Acelere una operación de Microsoft Ngen.exe, si es necesario

Una vez instaladas todas las actualizaciones de software, debe permitir a `Ngen.exe` básicamente recompilar código de bytes `.NET` en imágenes nativas y construir las entradas del registro para administrarlas.

`Ngen.exe` es el generador de imágenes nativas de Microsoft, que forma parte del sistema `.NET`. Windows determina cuándo se ejecuta `Ngen.exe` en función del software que se está instalando y de lo que detecta Windows en la configuración.

### Importante:

Cuando `Ngen.exe` se está ejecutando, debes dejar que se complete. Una operación `Ngen.exe` interrumpida puede ocasionar que los ensamblados `.NET` no funcionen o que haya otros problemas en el sistema `.NET`.

Normalmente, `Ngen.exe` es una operación en segundo plano que se detiene cuando hay actividad en primer plano. Si quieres acelerar una operación `Ngen.exe`, puede poner la tarea en primer plano para completarla lo antes posible.

Para poner la tarea en primer plano:

1. Abra un símbolo del sistema como Administrador.
2. Vaya al directorio `Microsoft.NET\Framework` de la versión actualmente en uso:  

```
cd C:\Windows\Microsoft.NET\FrameworkNN\vX.X.XXXXX
```
3. Introduzca el siguiente comando `Ngen.exe` para ejecutar todos los elementos en cola. Este comando procesa las instalaciones de componentes en cola antes de crear ensamblajes.

```
ngen eqi 3
```

La tarea `Ngen.exe` pasa al primer plano en la solicitud de comando y muestra los ensamblajes que se están compilando. Está bien si ve mensajes de compilación.

Puede utilizar el **Administrador de tareas** para ver si `MSCORSVW.EXE` se está ejecutando una instancia de. Si es así, permite que se complete o se ejecute `ngen update eqi 3`.

### Precaución:

No reinicie para detener la tarea. ¡Permita que la tarea se complete!

4. Asegúrese de que todos los procesos `Ngen.exe` se han ejecutado hasta su finalización.

## Preparar la imagen del sistema operativo para la disposición en capas en Nutanix

June 29, 2023

En este tema se explica cómo preparar una imagen limpia del sistema operativo para importarla en una nueva capa de SO. Antes de empezar, debe cumplir con los [requisitos](#). Mientras prepara la imagen, puede [acelerar una operación de Microsoft Ngen.exe, si es necesario](#), si cree que está tardando demasiado.

Si usa Windows 10 y *no* ejecuta PVS, Machine Creation o View, puede acelerar los tiempos de inicio del escritorio [eliminando las aplicaciones integradas de Windows 10](#). Sin embargo, recomendamos eliminar las aplicaciones en una *nueva versión* de la capa del sistema operativo, *no* en la propia imagen del sistema operativo.

### Nota:

No utilice un archivo desatendido en Nutanix. El software App Layering elimina el archivo de instalación desatendida si está presente, porque no es necesario o recomendado en Nutanix.

## Instalar el SO en una máquina virtual

Como parte de este procedimiento, puede configurar la activación del Servicio de administración de claves (KMS).

### Nota:

La publicación de imágenes en entornos en los que se utilizan KMS y la activación basada en Active Directory (ADBA) al mismo tiempo provoca problemas de activación.

1. Inicie sesión en la consola de Prism.
2. Seleccione **Tarea > VM** y cambie a **Vista de tabla** para ver las máquinas virtuales existentes.
3. Haga clic en **+Crear máquina virtual** en la esquina superior derecha e introduzca los detalles de la nueva máquina virtual:
  - a) Introduzca un **nombre** y agregue una **descripción**.
  - b) Seleccione la cantidad de **vCPU**.
  - c) Configure los **núcleos por CPU**.
  - d) Configure la **memoria**.
  - e) Seleccione **Discos** y cree una máquina virtual con tres discos. El primer CD-ROM es la ISO para el sistema operativo. El segundo CD-ROM es para los controladores Nutanix VIRTIO que permiten a la máquina virtual Nutanix acceder al disco donde se instala el sistema operativo. Se asigna un CD-ROM al principio.

- i. Modifique los valores del **CD-ROM** asignado:
    - ii. Para la operación, seleccione Clonar de un archivo **ADSF**.
    - iii. En Tipo de bus, seleccione **IDE**.
    - iv. Introduzca la ruta de acceso a su ISO de Windows. La ruta es la combinación del contenedor de almacenamiento y el nombre ISO. Por ejemplo:  
`/ISOStore/en_windows_10_enterprise_version_1511_x64_dvd_7224901.iso`
    - v. Haga clic en **Actualizar**.
  - f) Para agregar otro disco, haga clic en el botón **+Agregar disco nuevo**:
    - i. Configure el Tipo en **CDROM**.
    - ii. Configure la operación para **clonar desde un archivo ADSF**.
    - iii. Configure el tipo de bus en **IDE**.
    - iv. Introduzca la ruta de acceso a los controladores VIRTIO de Windows. Por ejemplo:  
`/ISOStore/virtio-win-0.1.102.iso`
    - v. Haga clic en **Agregar**.
  - g) Haga clic en el botón **+Agregar disco nuevo**.
    - i. Defina el **Tipo** en **Disco**.
    - ii. Configure la **operación** en **Asignar en contenedor**.
    - iii. Defina el **Tipo de bus** en **SCSI**.
    - iv. Seleccione el **contenedor** que quiera utilizar.
    - v. Introduzca el **tamaño**.
    - vi. Haga clic en **Agregar**.
  - h) Haga clic en **+Agregar nueva NIC** e introduzca el **nombre de la VLAN**.
  - i) Haga clic en **Guardar**.
4. Encienda la **máquina virtual**.
- a) Seleccione **Tareas > VM**.
  - b) Cambie a la **vista de tabla** para ver las máquinas virtuales existentes.
  - c) Seleccione la máquina virtual en la **tabla** y haga clic en **Encender**.
5. Inicie la consola seleccionando la máquina virtual y haciendo clic en Iniciar consola. Cuando se inicia la máquina virtual, comienza a instalar el sistema operativo Windows desde el disco ISO. Cuando se inicia la máquina virtual, comienza a instalar el sistema operativo Windows desde el disco ISO.
- a) Cuando se le preguntó: “¿Dónde quiere instalar Windows?”, observe que aunque haya agregado un disco en el asistente de creación de VM, no hay ningún disco.
  - b) Seleccione la opción **Cargar controlador** y, a continuación, seleccione **Examinar**.
  - c) Seleccione el CD con los controladores **virtio-win-0.1.1**.

- d) Seleccione la carpeta `vioscsi` y elija la carpeta para su sistema operativo Windows.
6. Después de instalar manualmente el sistema operativo, instale los controladores VirtIO:
  - a) Inicie el **Administrador de dispositivos**.
  - b) Seleccione **Otros dispositivos**, haga clic con el botón derecho en **Controlador Ethernet** y seleccione **Actualizar software del controlador**.
  - c) Busque **Mi PC** y seleccione el **CD de VirtIO**. Los controladores Ethernet se almacenan en la carpeta **NetKVM**.
7. **Sistema operativo de servidor:** Si necesita una función de alojamiento de sesión:
  - a) Seleccione **Agregar funciones y funciones**.
  - b) Para el tipo de instalación, seleccione **Instalación basada en funciones**.
  - c) Para el rol de servidor, seleccione **Servicios de escritorio remoto > Host de sesión de escritorio remoto**.
  - d) Complete el proceso de agregar roles de servidor.
8. Instale todas las actualizaciones importantes. Reinicie el sistema y compruebe si hay más actualizaciones. Algunas actualizaciones solo estarán disponibles después de instalar otras.
9. Instale todos los Service Packs necesarios.
10. Desactive la **restauración del sistema de Windows** y las **actualizaciones automáticas de Windows**.
11. Habilite el administrador integrado y marque **La contraseña no caduca nunca**.
12. Si utiliza licencias del Servicio de administración de claves (KMS), ejecute una ventana de comandos como Administrador e introduzca los siguientes comandos:

```
1 slmgr /skms <kmsserverhost>
2 slmgr /rearm
3 reboot
4 slmgr /ipk XXXX-YOUR-KMS-KEY-XXXX
5 slmgr /ato
6 <!--NeedCopy-->
```
13. **Sistema operativo de servidor:** Agregue usuarios de dominio a la configuración remota del sistema operativo del servidor.
14. Compruebe si hay NIC muertas (fantasmas) y elimine si existe alguna. Introduzca los comandos:

```
1 set devmgr_show_nonpresent_devices=1
2 devmgmt.msc
3 <!--NeedCopy-->
```
15. Desinstale las NIC muertas (fantasmas).
16. Si se trata de un SO de servidor, ejecute los siguientes comandos en PowerShell:

```
1 Set-ExecutionPolicy Unrestricted
2 Enable-PSRemoting
3 <!--NeedCopy-->
```

## Ejecute las herramientas de máquina del sistema operativo en la imagen del sistema operativo

Para preparar la imagen del sistema operativo para que se ejecute en una capa, ejecute el archivo de herramientas de máquinas del sistema operativo en la imagen. Este ejecutable ejecuta un script de configuración de GPO (gpsetup.cmd) y un script para establecer versiones de KMS (SetKMSVersion.hta).

1. Descargue el siguiente archivo ejecutable en la imagen del sistema operativo:

`Citrix_App_Layering_OS_Machine_Tools_20.x.x.exe`

2. Ejecute el ejecutable. Los archivos se guardan en:

`c:\windows\setup\scripts`

**Nota:**

El archivo debe extraerse al directorio `c:\windows\setup\scripts`. No cambie el directorio.

## Si utiliza el Servicio de administración de claves (KMS), configure la activación de licencias

Una vez extraídos los scripts, la utilidad SetKmsVersion le pide que elija si quiere utilizar la licencia de KMS.

**Nota:**

La publicación de imágenes en entornos en los que se utilizan al mismo tiempo la activación basada en KMS y la activación basada en Active Directory (ADBA) provoca problemas de activación.

1. En el cuadro de diálogo siguiente, seleccione si quiere utilizar las licencias del Servicio de administración de claves (KMS).





Para configurar scripts para KMS, haga lo siguiente.

1. Desplácese hasta:

`c:\windows\setup\scripts`

2. Ejecute **SetKMSVersion.exe** como administrador. Esto crea un script en la carpeta `c:\windows\setup\scripts\kmsdir`.

Cuando se inicia el sistema operativo, se ejecuta el script de activación de KMS apropiado.

### **Asegúrese de que estén instaladas las versiones correctas de .NET Framework (Windows 10 y Windows Server 2016)**

.NET Framework es un marco de software proporcionado por Microsoft y es necesario para que se ejecuten muchas aplicaciones de terceros. Todas las instalaciones de .NET Framework deben incluirse en la capa del sistema operativo. Esto incluye .NET 3.5 y .NET 4.0 o versiones posteriores.

**Nota:**

Citrix Virtual Apps and Desktops (CVAD) 2303 requiere .NET 4.8 para agregar VDA.

Asegúrese de instalar .NET Framework y cualquier actualización en su capa de sistema operativo.

### **Instalar los servicios App Layering**

1. En la carpeta `c:\windows\setup\scripts`, ejecute **setup\_x86.exe (32 bits)** o **setup\_x64.exe (64 bits)**.

2. La instalación solicita la ubicación del archivo `unattend`. NO utilice el archivo `unattend` en Nutanix.

### Ejecute el script de optimización, si utiliza MS Office

El script de optimización incluida en el paquete de instalación de App Layering es necesaria para crear capas en Microsoft Office. Este script le permite guardar memoria y CPU; para ello, inhabilita los servicios que no necesita, habilita los servicios que necesita y elimina los controladores y los parámetros específicos de la instalación.

Puede ejecutar el script de optimización en la capa de SO y, si es necesario, reemplazarlo con una nueva versión del script en una capa de aplicaciones incluida en la plantilla de imagen. Dado que las capas de la aplicación se aplican a la imagen después de la capa de SO, el script de la capa de aplicaciones anula la versión original de la capa de SO.

1. En la carpeta `c:\windows\setup\scripts`, ejecute el archivo `optimizations.cmd` para crear un archivo que se ejecute cuando se cree la imagen.
2. Siga las instrucciones para ejecutar `optimizations.cmd` en la imagen del sistema operativo.

### Acelere una operación de Microsoft Ngen.exe, si es necesario

Una vez instaladas todas las actualizaciones de software, debe permitir a `Ngen.exe` básicamente recompilar código de bytes `.NET` en imágenes nativas y construir las entradas del registro para administrarlas.

`Ngen.exe` es el generador de imágenes nativas de Microsoft, que forma parte del sistema `.NET`. Windows determina cuándo se ejecuta `Ngen.exe` en función del software que se está instalando y de lo que detecta Windows en la configuración.

#### Importante:

Cuando `Ngen.exe` se está ejecutando, debes dejar que se complete. Una operación `Ngen.exe` interrumpida puede ocasionar que los ensamblados `.NET` no funcionen o que haya otros problemas en el sistema `.NET`.

Normalmente, `Ngen.exe` es una operación en segundo plano que se detiene cuando hay actividad en primer plano. Si quieres acelerar una operación `Ngen.exe`, puede poner la tarea en primer plano para completarla lo antes posible.

Para poner la tarea en primer plano:

1. Abra un símbolo del sistema como Administrador.

2. Vaya al directorio `Microsoft.NET\Framework` de la versión actualmente en uso:

```
cd C:\Windows\Microsoft.NET\FrameworkNN\vX.X.XXXXX <!--NeedCopy
-->
```

3. Introduzca el siguiente comando `Ngen.exe` para ejecutar todos los elementos en cola. Este comando procesa las instalaciones de componentes en cola antes de crear ensamblajes.

```
ngen eqi 3 <!--NeedCopy-->
```

La tarea `Ngen.exe` pasa al primer plano en la solicitud de comando y muestra los ensamblajes que se están compilando. Está bien si ve mensajes de compilación.

Puede utilizar el **Administrador de tareas** para ver si `MSCORSVW.EXE` se está ejecutando una instancia de. Si es así, permite que se complete o se ejecute `ngen update eqi 3`.

**Precaución:**

No reinicie para detener la tarea. ¡Permita que la tarea se complete!

4. Asegúrese de que todos los procesos `Ngen.exe` se han ejecutado hasta su finalización.

## Crear la capa de SO

July 6, 2022

Una capa del sistema operativo incluye el software y la configuración del sistema operativo que implementa en imágenes en capas. La capa del sistema operativo es necesaria para crear:

- Capas de plataforma
- Capas de aplicaciones
- Imágenes en capas

**Importante:**

En la nueva interfaz de usuario, la única forma de crear una capa de sistema operativo es importarla con la utilidad `ImportOSLayer.ps1`. Ya no puede crear capas de SO a través de la consola de administración. Para obtener más información, póngase en contacto con su representante de Citrix.

## Acerca de la importación del sistema operativo de la capa

La única forma de importar el sistema operativo es ejecutar el script de importación del SO, incluido en la descarga de OS Machine Tools:

```
1 ImportOSLayer.ps1
2 <!--NeedCopy-->
```

Las ventajas de utilizar un script de importación incluyen:

- Mejor rendimiento: La importación del sistema operativo se ejecuta más rápido.
- Máquina con interfaz de firmware extensible unificada (UEFI) y soporte de arranque seguro.

### Requisitos

Antes de crear la capa del sistema operativo, asegúrese de:

- [Prepare la imagen del sistema operativo para importarla en la capa.](#)
- [Instale el dispositivo.](#)
- [Configurar App Layering.](#)

### Consideraciones para la capa del sistema operativo

- Para implementar parches y actualizaciones de Windows, simplemente puede agregar una versión a la capa. Puede volver fácilmente a la versión anterior de la capa, si es necesario.
- Puede seleccionar cualquier versión de la capa para utilizarla en una plantilla de imagen y, por lo tanto, en las imágenes publicadas.
- Puede actualizar el sistema operativo mediante Windows Update, Windows Server Update Services (WSUS) o paquetes de actualización independientes sin conexión. *No* utilice herramientas como SCCM.
- Las capas de plataforma y aplicación están vinculadas a la capa de SO específica que usa para crearlas, aunque no a una versión específica de la capa. Cuando agrega versiones a la capa del sistema operativo, las capas de aplicación y plataforma dependientes siguen funcionando.
- Las actualizaciones de Windows se deben aplicar a la capa del sistema operativo antes de actualizar cualquier otra capa.

### Importar el sistema operativo mediante el script ImportOSLayer.ps1

En este procedimiento se explica cómo importar el sistema operativo de la nueva capa de sistema operativo mediante el script `ImportOsLayer.ps1`.

Si ha descargado y ampliado App Layering OS Machine Tools en la imagen de su sistema operativo, `ImportOsLayer.ps1` se copia en `c:\windows\setup\scripts`.

## Ejecutar el script

Para importar el SO:

1. Ejecute el script de PoSH `ImportOsLayer.ps1` como administrador:

```
1 C:\Windows\Setup\scripts\ImportOsLayer.ps1 -ElmAddress <Ip Address
> [-IgnoreCertErrors]
2 C:\Windows\Setup\scripts\ImportOsLayer.ps1 -ElmAddress <FQDN> [-
IgnoreCertErrors]
3 <!--NeedCopy-->
```

donde

- `ElmAddress` es la dirección IP o el FQDN del dispositivo App Layering. Especifica dónde se crea la nueva capa del sistema operativo.
  - `IgnoreCertErrors` ignora los errores de certificación cuando el script se comunica con el dispositivo App Layering.
2. El script `ImportOsLayer.ps1` le solicita las credenciales para conectarse al dispositivo App Layering (denominado ELM en el script). El script utiliza sus credenciales para crear una sesión en el dispositivo.
  3. A continuación, el script le pedirá detalles sobre la nueva capa del sistema operativo:
    - `LayerName` (obligatorio)
    - `VersionName` (obligatorio)
    - `LayerSizeGib` (obligatorio, pero el valor predeterminado es 60 GB)
    - `LayerDescription` (opcional)
    - `VersionDescription` (opcional)
    - Comentario (opcional)

Una vez que haya introducido la información requerida, el script reinicia el sistema en el motor de composición, importa el sistema operativo y construye la capa. Supervise el progreso del trabajo en la consola de administración.

Cuando el motor de composición ha terminado (éxito o error), se reinicia de nuevo en la imagen del sistema operativo Windows.

## Crear capa de plataforma

May 9, 2024

Una capa de plataforma incluye el software de plataforma y la configuración necesaria para que sus capas e imágenes en capas se ejecuten sin problemas en su entorno.

Puede crear capas de plataforma para dos propósitos:

- **Para crear y empaquetar capas:** cuando haya importado el sistema operativo desde un hipervisor diferente al que creó las capas, utilice este tipo de capa de plataforma para crear capas de aplicaciones.
- **Para publicar imágenes en capas:** utilice este tipo de capa Platform en su plantilla de imagen para que las imágenes en capas publicadas se ejecuten sin problemas en su entorno.

### Capas de plataforma para empaquetar capas o publicar imágenes en capas

Utilice la siguiente tabla para determinar si necesita una capa de plataforma. Esta tabla también muestra qué software instalar en la capa de plataforma, si lo necesita.

|                                  | Capas de empaquetado                                                                                                                                                                                                                    | Publicación de imágenes en capas                                                                                                                                                |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ¿Se requiere capa de plataforma? | Necesario si la imagen del sistema operativo se originó en un Hypervisor diferente.<br>Cuando una aplicación requiere el agente o el software SSO, puede crear una capa de plataforma específicamente para crear y actualizar esa capa. | Necesario al publicar en un servidor de Provisioning y utilizar un agente de conexión.                                                                                          |
| Qué instalar                     | Herramientas de Hypervisor, cuando el sistema operativo se originó en un hipervisor diferente. El SSO o el software del agente, si es necesario para crear una capa de aplicación.                                                      | Software y configuración del agente de conexión y aprovisionamiento. Si publica en un Hypervisor diferente al del que se originó el SO, incluya las herramientas de Hypervisor. |
| Valores a seleccionar            | Seleccione su hipervisor.                                                                                                                                                                                                               | Seleccione el hipervisor, el software de Provisioning y el agente de conexiones.                                                                                                |
| Lo que necesitas                 | Instalador para el hipervisor                                                                                                                                                                                                           | Instaladores para el software de Provisioning y el broker de conexiones.                                                                                                        |

## Otros programas y ajustes para incluir en la capa de plataforma

Además del software de plataforma especificado anteriormente, debe incluir los siguientes ajustes y software en la capa de plataforma:

- Unirse al dominio
- Controladores NVIDIA, si procede
- Citrix Receiver, para el componente de inicio de sesión único
- Agente de Citrix Workspace Environment Management (WEM)

### Nota:

La clave RSA generada por Citrix WEM provoca problemas al utilizar WEM en la imagen implementada. Si la clave RSA está presente al finalizar la capa, aparece un mensaje que indica que debe eliminar el archivo de clave RSA, que comienza con la siguiente ruta: `C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18\fb8cc9e38d3e60ab60c17cdfd6dd6d99_`.

- Cualquier software que impacta la pila de inicio de sesión, por ejemplo, Imprivata
- Citrix Provisioning en Hyper-V: Requiere un adaptador de red heredado para el arranque PXE
- Software Microsoft System Center Configuration Manager (SCCM), si lo está usando

## Proceso para crear una capa de plataforma

Los pasos para crear una capa de plataforma son los siguientes:

1. Cree una capa de plataforma en la consola de administración.
2. Conéctese a la máquina de embalaje e inicie sesión en ella.
3. Instale el software del agente de Provisioning y conexión.
4. ¿Se ejecuta el dispositivo en un Hypervisor diferente al que se crean capas y se publican imágenes? En caso afirmativo, también recomendamos instalar las herramientas del hipervisor.
5. Verifique la capa y apague la máquina de empaquetado.
  - Si la configuración del conector seleccionada está configurada para usar **Composición de descarga**, la capa se finaliza automáticamente.
  - Si la configuración del conector *no* está establecida en **Descarga de composición**, [finalice la capa manualmente](#), como se describe en los pasos detallados de este artículo.

## Cuándo actualizar una capa de plataforma

La capa de plataforma es la capa de prioridad más alta. Es fundamental para implementar imágenes, especialmente para dispositivos de red. Siempre que actualice el software de infraestructura, agregue una versión a la capa de plataforma.

Cuando actualiza la capa del sistema operativo, la imagen a veces tiene problemas de inicio. Para solucionar el problema, agregue una versión a la capa de plataforma mediante la nueva capa del sistema operativo. Una vez que se inicie la máquina de empaquetado, apague la máquina para su finalización. La capa de plataforma reúne los componentes críticos de la nueva versión de la capa de sistema operativo y los actualiza en la plataforma para que coincidan con la versión del sistema operativo.

## Requisitos

Al crear una capa de plataforma, los instaladores de software deben estar disponibles en una ubicación a la que pueda acceder la máquina de empaquetado. Por ejemplo, el servidor de Provisioning y el software del agente de conexiones deben estar accesibles. Si el dispositivo se ejecuta en otro Hypervisor, incluya también las herramientas del hipervisor.

Para conocer los requisitos detallados, seleccione el entorno en el que crea capas o publica imágenes:

- [Machine Creation for Azure](#)
- [Machine Creation for Nutanix AHV](#)
- [Machine Creation for vSphere](#)
- [Creación de máquinas para XenServer](#)
- [Citrix Provisioning](#)
- [XenServer](#)
- [MS Azure](#)
- [MS Hyper-V](#)
- [Nutanix AHV](#)
- [VMware vSphere](#)
- [Recursos compartidos de archivos de red \(otras plataformas\)](#)

## Una palabra sobre optimizaciones

La capa de plataforma es la capa de prioridad más alta. Podría pensar que sería el mejor lugar para incluir optimizaciones. Sin embargo, en Windows 10, las optimizaciones que eliminan aplicaciones de Windows solo funcionan en la capa del sistema operativo. Las aplicaciones de Windows están integradas con la **Tienda** Windows, que solo se puede modificar en la capa del sistema operativo.



Citrix ofrece una excelente utilidad de optimización llamada [Citrix Optimizer](#). Se recomienda usar esta utilidad en lugar del optimizador incluido con App Layering, ya que Citrix Optimizer normalmente puede revertir las optimizaciones si es necesario.

Para acelerar los inicios de sesión de los usuarios. Inicie sesión con una cuenta de usuario de red y reinicie el escritorio. A continuación, inicie sesión como administrador y elimine el perfil creado. Cuando el primer usuario de red inicia sesión, algunos archivos del sistema se actualizan y, por lo general, el rendimiento de inicio de sesión mejora.

### Iniciar una nueva capa de plataforma

Para crear una capa de plataforma, siga estos pasos:

- Prepare la capa con **Crear capa de plataforma**.
- Implemente una máquina de empaquetado en su entorno.
- Instale las herramientas y configure la configuración de su entorno.
- Finalice la capa.

Siga estos pasos, comenzando en la barra de acciones:

1. Seleccione **Capas > Capas de plataforma**. A continuación, seleccione **Crear capa de plataforma**.
2. En la ficha Detalles de capa, introduzca un **Nombre de capa** y una **Versión**, ambos valores obligatorios. Si lo quiere, también puede introducir otros valores.
3. En la ficha Detalles de la versión:
  - a) (Necesario) Introduzca un nombre de nueva versión. Por ejemplo, introduzca la versión del software u otra información de identificación.
  - b) Si piensa agregar una versión a una capa existente, el campo **Versión base** le permite elegir qué versión usar como punto de partida. La opción predeterminada es la última versión.
4. En la ficha Capa de sistema operativo, seleccione la capa de SO que quiere asociar a esta capa de plataforma.
5. En la ficha Conector, elija una **configuración de conector** para la plataforma en la que va a crear esta capa.
6. En la ficha **Tipos de plataforma**, selecciona **Esta plataforma se utilizará para publicar imágenes en capas** o **Esta plataforma se utilizará para empaquetar**. A continuación, seleccione el hipervisor, el software de Provisioning y el agente de conexiones en el que va a publicar la imagen en capas.

**Nota:** Si *no* usas aprovisionamiento ni un agente de conexiones, selecciona **Ninguno** para cada una de esas opciones.

7. En la ficha Disco de empaquetado, introduzca un **nombre de archivo** para el disco de empaquetado. Este disco se utiliza para la máquina de empaquetado (la máquina virtual) donde quiere instalar las herramientas.
8. En la ficha Asignación de iconos, seleccione un icono para asignarlo a la capa. Este icono representa la capa del módulo Capas.
  - Para utilizar una imagen existente, seleccione una imagen en el cuadro de imagen.
  - Para importar una imagen nueva, haga clic en **Examinar** y seleccione una imagen en formato PNG o JPG.
  - Si la capa utiliza uno de los iconos suministrados y un conector con la opción **de composición de descarga** seleccionada, la máquina empaquetadora asigna un icono en función del contenido de la capa.
9. En la ficha Confirmar y completar, revise los detalles de la capa de aplicaciones, introduzca un comentario si es necesario y haga clic en **Crear capa**. Los comentarios que introduzca aparecerán en la vista **Información** del **Historial de auditoría**.
10. Seleccione la página **Tareas** y haga clic en la tarea **Empaquetar disco**. Haga clic en el icono de información para mostrar la descripción completa de la tarea.

Una vez creado el disco de empaquetado, la barra Tareas muestra la ubicación del disco de empaquetado en su entorno.

A continuación, puede implementar la máquina de empaquetado para su capa.

## Implementar una máquina de empaquetado

El sistema de App Layering crea una máquina de empaquetado en la ubicación definida en la configuración del conector. La máquina de empaquetado es una máquina virtual temporal donde se instala el software para la capa. Una vez finalizada la capa, se elimina la máquina de empaquetado.

### XenServer, Hyper-V, Nutanix AHV, VMware vSphere

El dispositivo crea la máquina de empaquetado en la ubicación definida en la configuración del conector.

1. Vaya a la consola de administración de App Layering y seleccione la página **Tareas**.
2. Abra la tarea Crear capa de plataforma para obtener el nombre de la máquina de empaquetado.
3. Inicie sesión en la consola de administración del hipervisor, por ejemplo: XenServer, Azure, Hyper-V, Nutanix o VMware.

4. Desde la consola del administrador del hipervisor, desplácese hasta la máquina de empaquetado. Si la máquina de empaquetado aún no está encendida, hágalo ahora.

### Citrix Provisioning para Hyper-V: configuración de dos tarjetas de red

Al usar tarjetas de red duales y ejecutar Citrix Provisioning para Hyper-V, debe configurar las tarjetas de la siguiente manera en *cada nueva versión de la capa Platform*.

Una vez que el software de aprovisionamiento esté instalado y se hayan completado los reinicios necesarios:

1. Abra un símbolo del sistema administrativo en la máquina de empaquetado.
2. Ejecute el comando: `ipconfig /all`
3. Haga coincidir la dirección IP de la NIC de transmisión (adaptador de red heredado en Hyper-V) con el nombre del adaptador correcto.
4. Renovar la concesión DHCP en la NIC de transmisión.
5. De nuevo en una línea de comandos administrativa, ejecute `ipconfig /release *adapter-name*` seguido de `ipconfig /renew *adapter-name*`. Este comando obliga a los controladores de App Layering a seleccionar este adaptador como la “NIC primaria” .
6. Ejecute **Shutdown for Finalize** y finalice la capa como lo haría normalmente.

Importante:

Si selecciona Apagar para finalizar, pero luego necesita volver a encender la máquina por cualquier motivo, debe volver a ejecutar los comandos de **liberación** y **renovación**.

### Azure

1. Vaya a la consola de administración de App Layering y seleccione la página **Tareas**. Abra la tarea *Crear capa de aplicaciones* y haga clic en el icono de información para ver los detalles.
2. Utilice el vínculo de los detalles de la tarea para desplazarse a la máquina de empaquetado de Azure. Se abrirá el panel Implementación personalizada.
3. Inicie sesión en el portal de Azure (<https://portal.azure.com>).
4. Establezca los parámetros de Azure.
  - Nombre de máquina de empaquetado: debe cumplir con los requisitos de nombre de máquina virtual de Azure.
  - Tamaño: tamaño de máquina virtual.
  - Red virtual y subred: para implementar la máquina de empaquetado.  
IMPORTANTE: Asegúrese de que el valor de la **ubicación del grupo de recursos** coincida con la **ubicación de la cuenta de almacenamiento** que configuró en la configuración del

conector. Si estas ubicaciones no son las mismas, la máquina de empaquetado no se puede implementar. Si la implementación falla, puede pegar el vínculo en el explorador de nuevo y comenzar de nuevo.

5. Una vez que la máquina de empaquetado esté encendida, puede instalar las aplicaciones que quiere incluir en la capa.

### **Cualquier otro hipervisor (a través del recurso compartido de archivos de red)**

1. Busque el disco de empaquetado en el directorio siguiente en el recurso compartido de archivos de red:

\Unidesk\Packaging Disks

2. Copie el disco de empaquetado en una ubicación independiente del hipervisor. Colocar el disco en otra ubicación permite espacio para los archivos generados por el hipervisor cuando crea una nueva máquina virtual.

**IMPORTANTE:** No copie el disco en la carpeta Finalizar hasta que esté listo para finalizar. Un disco de la carpeta Finalize no se puede conectar a la nueva máquina virtual que va a crear a continuación.

3. Cree una máquina virtual mediante el disco de empaquetado como disco de arranque.
4. Encienda la máquina de empaquetado.

Una vez que su máquina de empaquetado esté encendida, puede instalar sus herramientas de plataforma en la capa.

### **Instalar las herramientas de plataforma en la máquina de empaquetado**

A continuación, instale el software para la plataforma donde publica imágenes en capas. Las herramientas de la plataforma incluyen el Provisioning y el software de broker de conexión que requieren imágenes en capas en el entorno de destino. Tenga en cuenta que el estado del software cuando finalice la capa es el estado que utiliza la imagen.

1. Inicie sesión de forma remota en la máquina de envasado. Asegúrese de iniciar sesión con la cuenta de usuario que utilizó para crear el sistema operativo.
2. Instale las herramientas para las que están configuradas las imágenes en capas. Por ejemplo, incluya las herramientas de Provisioning, agente de conexiones e Hypervisor. No olvide los controladores, las aplicaciones de arranque y los archivos necesarios.
3. Si la instalación requiere un reinicio del sistema, reinicie manualmente. La máquina de empaquetado no se reinicia automáticamente.

4. Asegúrese de que la máquina de empaquetado esté en el estado en el que desea que esté cuando se inicie la imagen:
  - Si las herramientas que instale requieren alguna configuración o registro posterior a la instalación, siga estos pasos ahora.
  - Elimine los ajustes, las configuraciones, los archivos, las unidades asignadas o las aplicaciones que no desee incluir en la máquina de empaquetado.
5. (Opcional) Para personalizar la imagen implementada desde el ELM antes de la implementación en MCS, siga estos pasos:
  - a) Actualice sus herramientas maestras en la revisión 2308 del sistema operativo y versiones posteriores.
  - b) A continuación, crea el archivo:

```
c:\windows\setup\scripts\kmsdir\Admin_Controlled_Shutdown.txt
```

**Nota:**  
El contenido del archivo no es importante.
  - c) Cuando la imagen se implementa desde el ELM, la imagen iniciada permanece en ejecución para que pueda realizar sus personalizaciones. El reinicio no afecta al estado de la máquina.
  - d) Una vez que haya completado la personalización, ejecute el comando:

```
c:\windows\setup\scripts\kmsdir\CompleteDeployment.cmd.
```

En este punto, la máquina se apaga y finaliza la tarea de implementación. Con esto, puede implementar la máquina en MCS.

## Verifique la capa y apague la máquina de empaquetado

Una vez instaladas las herramientas en la máquina de empaquetado, puede verificar que la capa esté lista para finalizar. Debe completarse cualquier procesamiento posterior a la instalación que sea necesario. Por ejemplo, es posible que deba completarse un reinicio o un proceso `ngen` de Microsoft.

Para comprobar que los procesos pendientes están completos, ejecute la herramienta *Apagar para finalizar*. Busque el icono *Apagar para finalizar* en el escritorio de la máquina empaquetadora.

## Apague la máquina de empaquetado para que pueda finalizar la capa

1. Si no ha iniciado sesión en la máquina de empaquetado, inicie sesión remota mediante la cuenta configurada durante la creación de la capa de SO.
2. Haga doble clic en el icono *Apagar para finalizar*. Una ventana de línea de comandos muestra mensajes que detallan el proceso de verificación de capas.

3. Si hay una operación pendiente, se le pedirá que complete el proceso. Por ejemplo, si se debe completar una operación `ngen` de Microsoft, puede agilizar la operación `ngen`, tal como se detalla en la sección [Mensajes de integridad de las capas durante el proceso de finalización](#).
4. Una vez finalizadas las operaciones pendientes, vuelva a hacer doble clic en el icono *Apagar para finalizar*.

La capa ya está lista para finalizar.

- Si la configuración del conector seleccionada se establece en **Descarga de composición**, la capa se finaliza automáticamente.
- Si no está utilizando **la composición de descarga**, [finalice la capa manualmente](#).

### Mensajes de integridad de capa durante el proceso de finalización

Los siguientes mensajes de integridad de capa le indican qué operaciones en cola deben completarse antes de que la capa esté lista para finalizar:

- `A RunOnce script is outstanding - check and reboot the packaging machine.`
- `A post-installation reboot is pending - check and reboot the packaging machine.`
- `A Microsoft ngen operation is in progress in the background. - An MSI install operation is in progress - check the packaging machine.`
- `A reboot is pending to update drivers on the boot disk - check and reboot the packaging machine.`
- `A Microsoft ngen operation is needed.`
- `Software Center Client is configured to run, but the SMSCFG.INI is still present.` Para obtener más información sobre la implementación de SCCM en un entorno virtual, consulte el artículo de Microsoft TechNet [Implementing SCCM in a XenDesktop VDI environment](#).

Para obtener más información sobre el significado de los mensajes de integridad de capa y cómo depurarlos, consulte [Depuración de problemas de integridad de capas en Citrix App Layering 4.x y versiones posteriores](#).

No puede omitir los mensajes de integridad de capa apagando el equipo. El software App Layering lo devuelve a la máquina de empaquetado hasta que se hayan completado los procesos.

Si hay una operación `ngen` de Microsoft en curso, puede intentar acelerarla, como se describe en la sección siguiente.

## Agilizar las operaciones Ngen.exe de Microsoft, si es necesario

Una vez instaladas todas las actualizaciones de software, debe permitir a `Ngen.exe` básicamente recompilar código de bytes `.NET` en imágenes nativas y construir las entradas del registro para administrarlas.

El ejecutable `Ngen.exe` es el Generador de imágenes nativas de Microsoft, que forma parte del sistema `.NET`. Windows determina cuándo se ejecuta `Ngen.exe` en función del software que se está instalando y de lo que detecta Windows en la configuración.

### Importante:

Cuando `Ngen.exe` se está ejecutando, debes dejar que se complete. Una operación `Ngen.exe` interrumpida puede ocasionar que los ensamblados `.NET` no funcionen o que haya otros problemas en el sistema `.NET`.

Normalmente, `Ngen.exe` es una operación en segundo plano que se detiene cuando hay una actividad en primer plano. Para agilizar una operación `Ngen.exe`, coloca la tarea en primer plano para completarla.

Para poner la tarea en primer plano:

1. Abra un símbolo del sistema como Administrador.
2. Vaya al directorio `Microsoft.NET\Framework` de la versión actualmente en uso:

```
cd C:\Windows\Microsoft.NET\FrameworkNN\vX.X.XXXXX <!--NeedCopy
-->
```

3. Introduzca el siguiente comando `Ngen.exe` para ejecutar todos los elementos en cola. Este comando procesa las instalaciones de componentes en cola antes de crear ensamblajes.

```
ngen eqi 3 <!--NeedCopy-->
```

La tarea `Ngen.exe` pasa al primer plano de la línea de comandos y muestra una lista de los ensamblados que se están compilando. Está bien si ve mensajes de compilación.

Puede utilizar el **Administrador de tareas** para ver si `MSCORSVW.EXE` se está ejecutando una instancia de. Si es así, permite que se complete o se ejecute `ngen eqi 3`.

### Precaución:

No reinicie para detener la tarea. ¡Permita que la tarea se complete!

4. Asegúrese de que todos los procesos `Ngen.exe` se han ejecutado hasta su finalización.
5. Cuando termine, apague la máquina virtual con el acceso directo **Shutdown For Finalize** disponible en el escritorio.

## Finalizar la capa manualmente

La finalización de capa es más rápida cuando se utiliza un conector en uno de los hipervisores probados. Consulte la sección siguiente para obtener más información.

También puede finalizar una capa en otros hipervisores mediante el recurso compartido de archivos de red. Consulte la última sección de este artículo.

### XenServer, Azure, Hyper-V, Nutanix AHV, VMware vSphere

Ahora que la capa ha sido verificada y apagada, está lista para finalizar.

#### Hyper-V:

si está utilizando un conector con la opción **de composición de descarga** seleccionada, este proceso de finalización se automatiza y no tiene que seguir estos pasos manuales.

1. Vuelva a la consola de administración.
2. Seleccione **Capas > Capas de plataforma** y la versión de la capa en la ficha **Información de versión** que ha preparado.
3. Haga clic en **Finalizar** para terminar de crear la capa.
4. Supervise la barra de tareas para comprobar que la acción se ha completado correctamente.

Una vez verificada la capa, se retira la máquina de empaquetado para minimizar el espacio de almacenamiento utilizado.

### Cualquier otro hipervisor (a través del recurso compartido de archivos de red)

Ahora que la capa ha sido verificada y apagada, está lista para finalizar.

1. Copie el disco de empaquetado de la carpeta que contiene los archivos de la máquina de empaquetado a la carpeta Finalizar en el recurso compartido de archivos de red:  
\\Unidesk\Finalize
2. Vuelva a la consola de administración.
3. Seleccione **Capas > Capas de plataforma**.
4. Seleccione **Finalizar** en la barra de acciones.
5. Supervise la barra de tareas para comprobar que la acción se completa correctamente y que la capa se puede implementar.



## Crear o clonar una capa de aplicación

May 9, 2024

Una capa de aplicaciones es un disco virtual que incluye una o más aplicaciones. Normalmente, una capa de aplicación incluye una aplicación. Si incluye más de una aplicación en una capa, límitelo a elementos que normalmente actualice al mismo tiempo.

### Crear una capa de aplicación desde cero

Esta sección le guía a través de la creación de capas de aplicaciones, incluyendo:

- Requisitos y consideraciones
- Iniciar una nueva capa de aplicación
- Implementar la máquina de empaquetado
- Instalar la aplicación
- Mensajes de integridad de capa que puede ver
- Verifique la capa y apague la máquina
- Agilizar las operaciones [Ngen.exe](#) de Microsoft, si es necesario
- Finalizar la capa

### Requisitos y consideraciones

Una capa de aplicaciones incluye una o más aplicaciones y configuraciones relacionadas. Instale siempre MS Office en una capa de aplicaciones y nunca en la capa del sistema operativo.

- **Aplicaciones antivirus:** coloque siempre la aplicación antivirus en una capa de aplicaciones siguiendo las instrucciones que se proporcionan [aquí](#). Sea estratégico con las actualizaciones de los archivos de definición de virus. Además, tenga en cuenta las funciones de marcado de archivos, por ejemplo, Virtual Image Exception Tool de Symantec. Considere los motores de análisis basados en host y tenga en cuenta el retraso en el inicio de sesión del usuario. Asegúrese de escanear la imagen en capas publicada, no la capa. El análisis solo se realiza en el acceso de los usuarios en Citrix Virtual Apps y Citrix Virtual Desktops.
- **MS Office:** Use esta [receta](#) para instalar Office. Para las implementaciones de VDI de Office 2010 y versiones posteriores, considere KMS un requisito. Para Office 2007 y versiones anteriores, considere la concesión de licencias por volumen como requisito. Usar otras estructuras de licencias no es tan conveniente, ya que requieren que cada licencia se active en cada escritorio. Para conservar la configuración y los datos del usuario, habilite Office 365 User layer Stores.ost y archivos de streaming. Los índices de búsqueda no se almacenan.

- **Recetas para superponer ciertas aplicaciones:** Prácticamente cualquier aplicación se puede superponer, pero algunas son más fáciles de superponer si empiezas con los consejos que hemos reunido en nuestro foro de [Recetas de App Layering](#). Antes de comenzar, consulte el foro para obtener consejos y procedimientos sobre las aplicaciones específicas que está colocando en capas.
- **Aplicaciones que requieren que agregue un usuario o administrador local.** Los usuarios o administradores locales que se agregan o modifican al instalar una aplicación en una capa de aplicaciones no se mantienen. La capa del sistema operativo conserva los usuarios o grupos locales que agregue, pero las capas de la aplicación no lo hacen. Agregue el usuario local o el administrador a la capa del sistema operativo antes de instalar la aplicación, o considere la posibilidad de instalar la aplicación en la capa del sistema operativo.

### Iniciar una nueva capa de aplicación

Para crear una máquina de empaquetado donde pueda instalar la aplicación:

1. Inicie sesión en la consola de administración y seleccione **Capas > Capas de aplicaciones**.
2. Haga clic en **Crear capa** en la barra de **acciones**.
3. Introduzca un **nombre de capa** y una **versión**, ambos valores obligatorios. También puede introducir otros valores.
4. En la ficha Capa del SO, seleccione la capa del SO que quiere asociar a esta capa de aplicación.
5. (Opcional) La ficha Capas de requisitos previos le ofrece la opción de especificar otras capas de aplicaciones que deben estar presentes al instalar las aplicaciones en esta capa. Úselo solo cuando las aplicaciones requeridas no se puedan incluir en la misma capa. Para obtener más información sobre esta función avanzada, consulte Capas de requisitos previos en las siguientes secciones.  
**Nota:** Al agregar una nueva versión a una capa de aplicaciones existente, debe especificar las capas de requisitos previos que necesita. *No se transfieren de una versión a otra.*
6. En la ficha Conector, elija una configuración de conector que incluya las credenciales de la plataforma en la que planea crear la capa y la ubicación de almacenamiento. Si la configuración que necesita no aparece en la lista, haga clic en **Nueva** para [agregar](#) una.
7. En la ficha Disco de empaquetado, escriba un **nombre de archivo** para el disco de empaquetado y elija el formato del disco. Este disco se utiliza para la máquina de empaquetado, la máquina virtual donde se instala la aplicación.
8. En la ficha Asignación de iconos, elija un icono para asignarlo a la capa. Este icono representa la capa en el módulo Capas.
  - Para utilizar una imagen existente, seleccione una imagen en el cuadro de diálogo de la imagen.
  - Para importar una imagen nueva, haga clic en **Examinar** y seleccione una imagen en formato PNG o JPG.

- Si está usando un conector con la composición de descarga seleccionada y elige uno de los iconos que se incluyen con App Layering el equipo de empaquetado intentará asignar un icono basado en el contenido de la capa cuando se finalice la capa.
9. En la ficha Confirmar y completar, revise los detalles de la capa de aplicaciones y, a continuación, haga clic en **Crear capa**. Puede escribir un comentario opcional antes de crear la capa. Sus comentarios aparecen en la vista Información Historial de auditoría. Después de crear el disco de empaquetado, la barra de tareas muestra un enlace al disco de empaquetado en el hipervisor, donde puede implementar la máquina de empaquetado.
  10. Seleccione la página **Tareas** y haga clic en la tarea **Empaquetar disco**. Haga clic en el icono de información para mostrar la descripción completa de la tarea, incluido un enlace a la ubicación en la que está publicada la máquina empaquetadora de esta capa.

A continuación, puede implementar la máquina de empaquetado para su capa.

### Implementar la máquina de empaquetado

Seleccione su hipervisor:

- XenServer, Hyper-V, Nutanix o vSphere
- Azure
- Otro hipervisor (recurso compartido de archivos de red)

#### XenServer, Hyper-V, Nutanix, vSphere

1. Inicie sesión en el cliente de hipervisor (XenServer, Hyper-V Manager, Nutanix Prism o vSphere).
2. Inicie sesión en la consola de administración de App Layering y seleccione la página **Tareas** para ver las tareas actuales.
3. Seleccione la tarea **Crear capa de aplicaciones** y haga clic en el icono de información para ver la descripción completa de la tarea.
4. Utilice la dirección URL proporcionada en la descripción de la tarea para desplazarse a la máquina de empaquetado del cliente del hipervisor.
5. La máquina de empaquetado está encendida.

Ahora puede instalar las aplicaciones para esta capa en la máquina de empaquetado.

**Azure** El dispositivo abre la plantilla de *implementación personalizada* de Azure, en la que puede crear la máquina de empaquetado.

1. Inicie sesión en el portal de Azure (<https://portal.azure.com>). **Nota:** Debe iniciar sesión antes de realizar el siguiente paso.

2. Vaya a la consola de administración de App Layering y seleccione la página **Tareas**. Seleccione la tarea *Crear capa de aplicaciones* y haga clic en el icono de información para ver los detalles.
3. Utilice el vínculo de los detalles de la tarea para desplazarse a la máquina de empaquetado de Azure. Se abrirá el panel Implementación personalizada.
4. Establezca los parámetros de Azure.
  - Nombre de máquina de empaquetado: debe cumplir con los requisitos de nombre de máquina virtual de Azure.
  - Tamaño: tamaño de máquina virtual.
  - Red virtual y subred: para implementar la máquina de empaquetado.  
IMPORTANTE: Asegúrese de que el valor de la **ubicación del grupo de recursos** coincida con la **ubicación de la cuenta de almacenamiento** que configuró en la configuración del conector. Si estas ubicaciones no son las mismas, la máquina de empaquetado no se puede implementar. Si la implementación falla, puede pegar el vínculo en el explorador de nuevo y comenzar de nuevo.
5. Una vez que la máquina de empaquetado esté encendida, puede instalar la aplicación que quiere incluir en la capa.

### Otro hipervisor (mediante el recurso compartido de archivos de red del dispositivo)

1. Busque el disco de empaquetado en el directorio siguiente en el recurso compartido de archivos de red:  
\\Unidesk\Packaging Disks
2. Copie el disco de empaquetado en una ubicación independiente del hipervisor. Esto deja espacio para los archivos generados por el hipervisor cuando usa el disco para crear una nueva máquina virtual.  
**Importante:** No copie el disco en la carpeta Finalizar hasta que esté listo para finalizar. Un disco de la carpeta Finalize no se puede conectar a la nueva máquina virtual que va a crear a continuación.
3. Cree una máquina virtual mediante el disco de empaquetado como disco de arranque.
4. Encienda la máquina de empaquetado.

Una vez que la máquina de empaquetado esté encendida, puede instalar la aplicación que quiere incluir en la capa.

### Instalar la aplicación

Cuando instale su aplicación en la máquina de empaquetado, deje la aplicación como quiera que los usuarios la vean cuando inicien sesión. El estado de la aplicación es lo que experimentan los usuarios cada vez que acceden a la aplicación.

1. Inicie sesión de forma remota en la máquina empaquetadora con la *cuenta de usuario* utilizada para crear el sistema operativo.
2. Instale la aplicación, junto con los controladores, aplicaciones de nivel de arranque o archivos necesarios para la aplicación.
3. Si es necesario reiniciar el sistema, reiniciarlo manualmente. La máquina de empaquetado *no* se reinicia automáticamente. Si la aplicación que instala afecta a los componentes de nivel de arranque, reinicie la máquina de empaquetado como parte de finalizar la capa.
4. Asegúrese de que la máquina de empaquetado esté en el estado en el que quiere que esté para el usuario:
  - Si la aplicación requiere alguna configuración o registro posterior a la instalación, complete estos pasos ahora.
  - Elimine los ajustes, las configuraciones, los archivos, las unidades asignadas o las aplicaciones que *no* desee incluir en la máquina de empaquetado.

### Verifique la capa y apague la máquina

Una vez que la aplicación esté instalada en la máquina de empaquetado, verifique que la capa esté lista para ser finalizada. Una capa está lista para finalizarse cuando se complete todo el proceso posterior a la instalación.

Para comprobar que todos los procesos pendientes están completos, puede ejecutar la herramienta **Shutdown For Finalize** en el escritorio de la máquina de envasado.

Para utilizar la herramienta Apagar para finalizar:

1. Si no ha iniciado sesión en la máquina de empaquetado, inicie sesión remota como el usuario que creó la máquina.
2. Haga doble clic en el icono **Apagar para finalizar**. Una ventana de línea de comandos muestra mensajes que detallan el proceso de verificación de capas.
3. Si hay una operación pendiente que debe completarse antes de que se pueda finalizar la capa, se le pedirá que complete el proceso. Si es necesario completar una operación **Microsoft Ngen.exe**, es posible que pueda agilizar la operación **Ngen.exe**, tal y como se detalla más adelante en este artículo.
4. Una vez completadas las operaciones pendientes, vuelva a hacer doble clic en el icono **Apagar para finalizar**. Esto apaga la máquina de empaquetado y la capa está lista para finalizar.

### Mensajes de integridad de capa que pueden aparecer durante el proceso de finalización

Los siguientes mensajes de integridad de capa le indican qué operaciones en cola deben completarse antes de que la capa esté lista para finalizar:

- Un script de RunOnce es excepcional: compruebe y reinicie la máquina de empaquetado.
- Un reinicio posterior a la instalación está pendiente: compruebe y reinicie la máquina de empaquetado.
- Una operación de Microsoft Ngen.exe está en curso en segundo plano.
- Una operación de instalación de MSI está en curso: compruebe la máquina de empaquetado.
- Hay un reinicio pendiente para actualizar los controladores en el disco de arranque: verifique y reinicie la máquina de empaquetado.
- Se necesita una operación de Microsoft Ngen.exe.
- Software Center Client está configurado para ejecutarse, pero el archivo SMSCFG.INI sigue presente. Para obtener más información sobre la implementación de SCCM en una capa, consulte el artículo [App Layering Recipe: How to deploy Microsoft SCCM in a layer](#).

Para obtener más información sobre el significado de los mensajes de integridad de capa y cómo depurarlos, consulte [Depuración de problemas de integridad de capas en Citrix App Layering](#).

No puede omitir los mensajes de integridad de capa apagando la máquina, porque el software de App Layering se detiene y le devuelve a la máquina de empaquetado hasta que se hayan completado todos los procesos.

Si una operación de Microsoft Ngen.exe está en curso, es posible que pueda acelerarla, como se describe en la siguiente sección.

### **Agilizar las operaciones Ngen . exe de Microsoft, si es necesario**

Una vez instaladas todas las actualizaciones de software, debe permitir a `Ngen . exe` básicamente recompilar código de bytes `.NET` en imágenes nativas y construir las entradas del registro para administrarlas.

`Ngen . exe` es el generador de imágenes nativas de Microsoft, que forma parte del sistema `.NET`. Windows determina cuándo se ejecuta `Ngen . exe` en función del software que se está instalando y de lo que detecta Windows en la configuración.

#### **Importante:**

Cuando `Ngen . exe` se esté ejecutando, debe dejar que se complete. Una operación `Ngen . exe` interrumpida puede ocasionar que los ensamblados `.NET` no funcionen o que haya otros problemas en el sistema `.NET`.

Normalmente, `Ngen . exe` es una operación en segundo plano que se detiene cuando hay una actividad en primer plano. Si quieres acelerar una operación `Ngen . exe`, puede poner la tarea en primer plano para completarla lo antes posible.

Para poner la tarea en primer plano:

1. Abra un símbolo del sistema como Administrador.

2. Vaya al directorio `Microsoft.NET\Framework` de la versión actualmente en uso:

```
cd C:\Windows\Microsoft.NET\FrameworkNN\vX.X.XXXXX <!--NeedCopy
-->
```

3. Introduzca el siguiente comando `Ngen.exe` para ejecutar todos los elementos en cola. Este comando procesa las instalaciones de componentes en cola antes de crear ensamblajes.

```
ngen eqi 3 <!--NeedCopy-->
```

La tarea `Ngen.exe` pasa al primer plano de la línea de comandos y muestra una lista de los ensamblados que se están compilando. Está bien si ve mensajes de compilación.

Puede utilizar el **Administrador de tareas** para ver si `MSCORSVW.EXE` se está ejecutando una instancia de. Si es así, permite que se complete o se ejecute `ngen eqi 3`.

**Precaución:**

No reinicie para detener la tarea. ¡Permita que la tarea se complete!

4. Asegúrese de que todos los procesos `Ngen.exe` se han ejecutado hasta su finalización.
5. Cuando termine, apague la máquina virtual con el acceso directo **Shutdown For Finalize** disponible en el escritorio.

## Finalizar la capa

Una vez instalado el software y la máquina de empaquetado ha sido verificada y apagada, está listo para finalizar la capa.

**Hyper-V:**

si se **selecciona Descargar composición** en la configuración del conector, la finalización se produce automáticamente como parte del proceso de composición.

**XenServer, Azure, Hyper-V, Nutanix AHV, VMware vSphere** Ahora que la capa ha sido verificada y apagada, está lista para finalizar.

**Hyper-V:**

si está utilizando un conector con la opción **de composición de descarga** seleccionada, este proceso de finalización se automatiza y no tiene que seguir estos pasos manuales.

1. Vuelva a la consola de administración.
2. Seleccione **Capas > Capas de aplicaciones** y la capa que preparó.
3. Seleccione la versión de la capa en la ficha **Información de versión** y haga clic en **Finalizar** en la barra Acción.

4. Haga clic en **Finalizar** para terminar de crear la capa.
5. Supervise la barra de tareas para comprobar que la acción se ha completado correctamente.

Una vez verificada la capa, se retira la máquina de empaquetado para minimizar el espacio de almacenamiento utilizado.

**Otro hipervisor (recurso compartido de archivos de red)** Ahora que la capa ha sido verificada y apagada, está lista para finalizar.

1. Copie el disco de empaquetado de la carpeta que contiene los archivos de la máquina de empaquetado a la carpeta Finalizar en el recurso compartido de archivos de red:  
\\Unidesk\Finalize
2. Vuelva a la consola de administración.
3. Seleccione **Capas > Capas de aplicaciones**.
4. Seleccione la versión de la capa en la ficha **Información de versión** y haga clic en **Finalizar** en la barra Acción.
5. Supervise la barra de tareas para comprobar que la acción se completa correctamente y que la capa se puede implementar.

## Clonar una capa de aplicación

Puede crear una capa de aplicación que sea la misma que una capa existente clonando una versión específica de la capa. Durante el proceso de clonación, se le pedirá información específica de la capa. Puede actualizar la capa de aplicaciones agregando versiones a la misma. Dado que solo se clona una versión de una capa, la nueva capa tiene solo una versión para comenzar, incluso si la capa desde la que se clonó tenía muchas.

Para clonar una capa:

1. Seleccione la capa de aplicación que desee copiar y haga clic en **Clonar capa** en la barra de acciones.
2. Seleccione la versión de la capa de origen que quiere clonar. Puede elegir la versión que quiera en el menú desplegable.
3. Introduzca un nombre para la capa y una descripción si la información adicional es útil. Las descripciones son opcionales.
4. Introduzca la versión y una descripción de la versión, si la información adicional es útil.
5. En la ficha Asignación de iconos, seleccione el icono de la nueva capa.
6. En la ficha Confirmar y clonar, compruebe la configuración y haga clic en el botón **Clonar capa**.



Se crea una nueva capa con las mismas propiedades de capa que el origen, excepto el icono. La **prioridad** de la capa es mayor que la de la capa de origen, porque cada nueva capa de aplicaciones tiene una prioridad más alta que la última capa de aplicaciones creada. El nuevo tamaño de capa podría ser más pequeño que el original, pero esto solo indica que se eliminó el espacio vacío durante la clonación. La capa funciona igual que la fuente.

Puede usar la nueva capa como cualquier otra capa y *no* está asociada de ninguna manera a la capa original.

### Opciones avanzadas de capa de aplicaciones

Al crear y actualizar capas de aplicaciones, tenga en cuenta las siguientes funciones avanzadas.

- Script de capa personalizada
- Almacenamiento en caché de capas
- Capas de requisitos previos

#### Script de capa personalizada

Puede incluir un script en una capa de aplicación que se ejecute una vez, al iniciar el sistema. Para configurar el script, modifique las propiedades de la capa de aplicación.

**Nota:**

También puede modificar las propiedades de la revisión de la capa mientras se crea la revisión o incluso una vez finalizada.

El script se ejecuta la primera vez que se inicia cualquier imagen en capas que incluya la capa de aplicación. Si la capa de aplicaciones tiene capas elásticas, el script de capa personalizada se ejecuta al montar el disco de la capa de aplicaciones. Los scripts de capa personalizados se utilizan normalmente para aplicaciones, como MS Office, que requieren la activación de la licencia la primera vez que se inician.

**Edit Layer**  
CSG Sample Layer

Layer Name  
CSG Sample Layer

Layer Description  
Layer Description

Choose an Icon  
[Icon] ▼  
Upload a new icon: [Browse](#)

Script Path  
Script Path

**App Layer Settings**

Enable Elastic Layer Compatibility  
Choose this setting only if you are having problems using this layer elastically. This is unrelated to Elastic Fit and will not improve the Elastic Fit of the layer.  
[Elastic Layering Help](#)

Allow this App Layer to be elastically assigned to all Layered Images, regardless of OS layer

**Versions**

| Name          | Description         |
|---------------|---------------------|
| First Version | Version Description |

Confirm and Complete Cancel

### Almacenamiento en caché de capas para crear capas de aplicaciones más rápido

Puede utilizar el almacenamiento en caché de capas para acelerar los tiempos de creación de capas.

**Cómo funciona el almacenamiento en caché** La primera vez que crea una capa de aplicaciones, si el tamaño de la caché se establece en un valor lo suficientemente grande, se guarda en la caché una plantilla compuesta por el disco de arranque y el disco de empaquetado vacío. El disco de arranque incluye la capa del sistema operativo, la capa Plataforma y la capa Requisito previo (si la hay) que se especifican en la configuración de la capa de la aplicación.

Cada vez que crea una capa de aplicación que utiliza la misma combinación de capa de SO, capa de requisitos previos y capa de plataforma, el software de App Layering reutiliza la plantilla, lo que reduce significativamente el tiempo de creación.

Si, a continuación, crea una capa de aplicación que utiliza una capa de SO diferente, una capa de requisitos previos y una combinación de capas de plataforma, el software de App Layering crea una plantilla y la agrega a la caché.

**Tamaño de caché recomendado** El tamaño de caché recomendado depende del número de combinaciones de capas de SO, Plataforma y Requisitos previos que necesite para las capas de la aplicación. El número de combinaciones determina el número de plantillas guardadas en la caché.

Para estimar el espacio necesario para cada plantilla:

1. Seleccione el icono **i** para cada capa de sistema operativo, plataforma y requisito previo, y busque el **tamaño máximo de capa**.
2. Agregue los tamaños máximos de disco. El total es el tamaño de caché que necesita para esa plantilla.

Para estimar el espacio necesario para la caché, agregue el tamaño que determinó para cada una de las plantillas.

### Capas de requisitos previos

Las capas de requisitos previos, *rara vez* recomendadas, permiten incluir una o más capas de aplicaciones existentes en el disco de empaquetado al crear una capa o agregarle una versión.

Utilice capas de requisitos previos *solo si son necesarias*, ya que pueden agregar algo a la capa que no sea necesario para implementar la aplicación actual. Este comportamiento puede causar conflictos en el futuro.

**Cuándo utilizar las capas de requisitos previos** Las capas de requisitos previos se pueden requerir por varias razones:

- Al instalar la aplicación en la capa actual requiere la presencia de otra aplicación. Por ejemplo, cuando instala una aplicación que requiere Java, y Java se encuentra en una capa separada.
- Cuando la instalación del software agrega configuraciones a una aplicación existente. Por ejemplo, cuando instala un complemento de Office, primero debe instalar Microsoft Office.
- Cuando dos aplicaciones cambian la misma clave del Registro, y la segunda aplicación debe agregar a una clave y no reemplazarla. Por ejemplo, dos aplicaciones que cambian las claves de inicio de sesión en Windows, como Citrix Agent e Imprivata.

#### Nota

Algunos de estos problemas también se pueden manejar colocando las dos aplicaciones en la misma capa en lugar de usar capas de requisitos previos.

**Funciones de capa de requisitos previos** Las capas de requisitos previos tienen las siguientes funciones:

- Las capas de requisitos previos *no se incluyen* en la capa de aplicaciones que se utilizan para crear.
- La capa de aplicaciones que cree y cada una de sus capas de requisitos previos deben usar la misma capa de sistema operativo.
- Al agregar una *versión* a una capa de aplicación, las capas de requisitos previos *no se incluyen* de forma predeterminada. Cada vez que agregue una versión a una capa, debe seleccionar una o varias capas Requisitos previos.

## Aplicaciones antivirus de las capas

February 29, 2024

Este artículo proporciona las directrices fundamentales para implementar software antivirus en un entorno de App Layering o [User Personalization Layer \(UPL\)](#).

Para obtener más información específica sobre el antivirus, consulte la documentación del proveedor para las implementaciones de VDI.

### Recomendaciones para todos los programas antivirus

Cree una nueva capa de aplicaciones para instalar y mantener la solución antivirus que haya elegido. Citrix no recomienda instalar el software antivirus directamente en una capa de sistema operativo, ya que esto dificulta el mantenimiento y, a menudo, provoca la contaminación del estado del antivirus entre las capas empaquetadas de aplicaciones y plataformas.

#### Nota:

Esto no se aplica a las imágenes UPL en las que es necesario instalar el software antivirus en la imagen base.

Los siguientes son los puntos clave comunes a la mayoría de las implementaciones de antivirus en capas de aplicaciones (algunos también se aplican a la UPL):

- Si ya ha instalado el software antivirus en su capa de sistema operativo, debe desinstalarlo y volver a instalarlo en una nueva capa de aplicaciones.
  - Windows Defender es una excepción a este consejo de capas y los filtros integrados en el software App Layering y UPL evitan automáticamente que contamine otras capas.
- Evite combinar otras aplicaciones con software antivirus en la misma capa de aplicaciones.
- Siga las instrucciones del proveedor para la implementación de VDI (incluida la UPL).

- Considere la posibilidad de deshabilitar las actualizaciones automáticas del software antivirus principal. Estas actualizaciones se gestionan mejor mediante revisiones de la capa de aplicaciones o, con UPL, copias de seguridad de la imagen base.
- Las actualizaciones diarias de las definiciones de virus están bien y no deben verse afectadas por la desactivación de las actualizaciones principales.
- Agregue un archivo [UserExclusion](#) a la capa antivirus para impedir que los archivos y directorios persistan en las capas de usuarios (incluso para UPL). Consulte las directrices del proveedor de antivirus para las implementaciones de VDI no persistentes para ver los archivos o las carpetas que no deben conservarse.
- Agregue las exclusiones de registro recomendadas por el proveedor a la capa antivirus (incluida la UPL). Son relativamente poco frecuentes, pero si es necesario, póngase en contacto con el servicio de asistencia de Citrix.

En general, Citrix recomienda crear una nueva versión de la capa de aplicaciones cuando el software antivirus tenga una actualización importante. Una vez que la capa se haya actualizado, asígnela a todas las plantillas que utilizan esa aplicación antivirus y vuelva a implementar imágenes nuevas para aprovechar los cambios en el software antivirus.

Las imágenes publicadas, incluidas las imágenes maestras de UPL, se pueden iniciar fuera del entorno de escritorio para permitir el análisis previo del antivirus de la imagen ensamblada, según el software antivirus utilizado.

### **La capa elástica no está habilitada**

Si está implementando imágenes sin capas elásticas habilitadas, considere si las imágenes no son persistentes o persistentes:

En el caso de las máquinas persistentes, es posible que desee habilitar las actualizaciones automáticas para mantener actualizado el software antivirus.

En el caso de las máquinas no persistentes, es posible que no desees activar las actualizaciones automáticas, ya que las actualizaciones se producen en las imágenes después de cada reinicio. (La máquina no persistente se revierte cuando se reinicia.)

## **Instrucciones sobre App Layering**

January 12, 2024

Puede superponer la mayoría de las aplicaciones sin problemas, pero hay algunas que requieren un cuidado adicional.

- **Aplicaciones antivirus:** para obtener instrucciones detalladas, consulta la sección sobre [capas de aplicaciones antivirus](#).
- **Guía de aplicaciones para implementaciones de VDI:** para las pocas aplicaciones que requieren orientación especial en entornos virtuales, ofrecemos pasos más detallados en un foro de soporte en línea, denominado [recetas de la capa de aplicación](#).

## Recetas populares de App Layering

La siguiente lista incluye una muestra de recetas para las pocas aplicaciones que requieren guía de capas. A menos que se indique lo contrario, estas recetas se aplican a todas las versiones de App Layering

Si su aplicación no aparece en el [foro de recetas de la capa de aplicación](#), lo más probable es que pueda instalarla en una capa sin ninguna orientación especial.

- [Adobe Reader](#)
- [AppSense](#)
- [Bit9](#)
- [Chrome](#)
- [Dropbox](#)
- [Firefox](#)
- [Servidor de licencias IBM SPSS 21](#)
- [Java](#)
- [MS Office, incluido Office 365](#)
- [NVIDIA GRID](#)
- [Servidor de impresión](#)
- [QuickBooks](#)
- [Cliente de SCCM 2012](#)

## Implementar capas de aplicaciones como capas elásticas

February 29, 2024

Con la función de capas elásticas, puedes entregar aplicaciones con un objetivo limitado fuera de la imagen base. De hecho, puede asignar capas a usuarios específicos a petición. Con la configuración de capa elástica habilitada en una plantilla de imagen, los usuarios que inicien sesión en las imágenes publicadas pueden asignarse capas de aplicación específicas como capas elásticas.

## Acerca de las capas elásticas

Una *capa elástica* es una capa de aplicación que se asigna a usuarios y grupos individuales para la entrega bajo demanda. Los usuarios reciben las capas elásticas que se les asignan además de las aplicaciones incluidas en la imagen base.

Las capas elásticas le permiten ofrecer a cada usuario un conjunto único de aplicaciones junto con las aplicaciones comunes incluidas en la imagen base. En los hosts de sesión, se utiliza una capa elástica en todas las sesiones. En escritorios independientes, las capas elásticas se utilizan en grupos flotantes y grupos compartidos.

En función de los derechos de usuario, las capas elásticas se entregan a los escritorios de los usuarios al iniciar sesión. Puede asignar capas elásticas a los usuarios en hosts de sesión y también en escritorios independientes, siempre y cuando las imágenes se publicaran mediante App Layering.

## Asignaciones de capa elástica

Puede entregar una versión específica de la capa de aplicaciones a los miembros de un grupo cada vez que inicien sesión en sus escritorios. La versión de la capa de aplicaciones se asigna como una capa elástica. A continuación, se almacena una copia de la capa en el recurso compartido de archivos de red del dispositivo y se entrega a demanda a los usuarios y grupos de AD asignados, además de las capas que reciben a través de la imagen base.

Para usar esta función, agregue *Elastic Assignments* especificando qué usuarios y grupos reciben cada una de las capas de aplicaciones. A continuación, publique su imagen base con la configuración de **Elastic Layering** habilitada.

## Cómo los usuarios acceden a capas elásticas asignadas a ellas

Cuando los usuarios inician sesión en su sesión o escritorio, los iconos de sus capas elásticas aparecen como atajos en el escritorio.

Un usuario recibe una capa elástica en los siguientes casos:

- Al usuario (un usuario de AD en la consola de administración) se le asigna la capa.
- A un grupo de AD al que pertenece el usuario se le asigna la capa.
- Un equipo en el que el usuario inicia sesión es miembro de un grupo de AD que recibe la capa elástica.
- Un equipo en el que el usuario inicia sesión está asociado a un grupo de AD que se asigna a la capa a través de la consola de administración.

### **Cuando se asigna a un usuario más de una versión de una capa**

Cuando una capa se asigna directamente a un usuario, e indirectamente a uno o varios de los grupos de usuarios, reciben la versión más reciente asignada directamente. Por ejemplo:

- Si al usuario se le asigna la **versión 2** y a un grupo al que pertenece el usuario se le asigna la **versión 3**, el usuario obtiene la **versión 2**.
- Si a dos o más grupos a los que pertenece el usuario se les asignan versiones diferentes de la misma capa, el usuario recibirá la versión más reciente de la capa asignada.

### **Cuando un usuario recibe una capa de aplicación tanto en la imagen base como en una capa elástica**

Cuando se incluye una capa de aplicación en la imagen base, no la asigne al mismo usuario que una capa elástica. Si el usuario termina con la misma capa asignada en ambas direcciones, recibirá la capa elástica, independientemente de la versión.

### **Requisitos previos**

- .NET Framework 4.5 es necesario en cualquier imagen en capas donde las capas elásticas estén habilitadas.
- Las capas de aplicaciones que desea asignar como capas elásticas.

### **Consideraciones**

#### **Capas de aplicaciones con la misma capa de SO que la imagen en capas**

Para obtener los mejores resultados, al asignar capas de aplicaciones como capas elásticas, puede asignar capas de aplicaciones que tengan la misma capa de sistema operativo que la que se usa en la imagen en capas. Sin embargo, con este enfoque tradicional, es posible que necesite crear y administrar copias adicionales de algunas capas de aplicaciones, una para cada capa de sistema operativo con la que implemente.

#### **Cambio de capa de SO para capas elásticas**

Para asignar una capa elástica a los usuarios de una imagen en capas que utilice una capa de sistema operativo diferente, debe habilitar esta capacidad en las propiedades de la capa de aplicación activando la casilla de verificación **Permitir que esta capa de aplicaciones se asigne de forma elástica a todas las imágenes en capas, independientemente de la capa de sistema operativo**. Todas las limitaciones de capas elásticas son válidas al cambiar las capas del sistema operativo.



**Cuándo podría funcionar bien** Para aplicaciones sencillas que se pueden instalar en cualquier sistema operativo.

Ejemplo: Notepad++, WinRAR, 7Zip

**Cuando puede que no funcione bien** Para aplicaciones complejas cuya instalación depende del sistema operativo instalado.

Ejemplo:

- Si usa una capa de sistema operativo Windows 10 para crear la capa de aplicaciones y la imagen asignada como capa de sistema operativo Server 2019, es posible que la aplicación no funcione según lo esperado.
- Es posible que las aplicaciones que dependen de una versión específica de .Net no se ejecuten correctamente si el nuevo sistema operativo no tiene instalada la versión correcta de .Net.

**Nota:**

- Se recomienda utilizar la misma clase de sistema operativo y revisiones de sistema operativo que estén cerca unas de otras. Ejemplo: puedes usar dos revisiones de Windows 10 22H2 con una semana de diferencia.
- Cuando utilice una imagen de sistema operativo diferente, debe validar las capas que está asignando de forma elástica a cualquier usuario. Si las capas no se validan, debe crear una capa de aplicación con la capa del sistema operativo que se utiliza para la imagen y asignar las capas al usuario sin seleccionar la casilla de verificación **Permitir que esta capa de aplicaciones se asigne de forma elástica a todas las imágenes en capas, independientemente de la capa del sistema operativo.**
- Al agregar versiones a una capa de aplicación, debe usar la capa de SO incluida en la capa de aplicación original.

### **Limitaciones de capas elásticas**

No puede utilizar una capa elástica para lo siguiente:

- Microsoft Office, Office 365, Visual Studio.
- Aplicaciones con controladores que utilizan el almacén de controladores. Ejemplo: un controlador de impresora.
- Aplicaciones que modifican el hardware o la pila de red. Ejemplo: un cliente VPN.
- Aplicaciones que tienen controladores de nivel de arranque. Ejemplo: un antivirus.

Una capa de aplicaciones *no* conserva un usuario o administrador local que se agrega para una aplicación que lo requiere, pero la capa de SO sí. Por lo tanto, agregue el usuario local o el administrador a la capa del sistema operativo antes de instalar la aplicación. Una vez que la capa de la aplicación esté funcionando, puede asignarla como una capa elástica.

## Modo de compatibilidad de capas elásticas

Cuando un usuario inicia sesión en un escritorio provisionado con una imagen en capas, la capa elástica se compone en la imagen después de que el usuario inicia sesión. Si una capa elástica no se carga correctamente, intente habilitar el **modo de compatibilidad de capas elásticas**. Con el modo de compatibilidad activado, la capa elástica comienza a cargarse antes de completar el inicio de sesión.

### Importante:

El modo de compatibilidad es obligatorio cuando se utilizan aplicaciones publicadas, ya que la capa debe montarse antes del lanzamiento. De lo contrario, recomendamos inhabilitar el modo de compatibilidad, a menos que una capa elástica no funcione como se esperaba. Habilitar esta configuración en demasiadas capas ralentiza los tiempos de inicio de sesión.

## La cuenta de usuario bajo la que se ejecutan las capas elásticas

De forma predeterminada, cuando el primer usuario asignado a una capa elástica inicia sesión en su escritorio, se montan todas las capas elásticas asignadas al usuario. Otros usuarios que inician sesión en el equipo que aloja las capas utilizan la misma conexión que el primer usuario. La conexión dura 10 horas después del primer inicio de sesión, y luego todas las capas elásticas se desconectan. En un entorno basado en turnos, los usuarios en el segundo turno se verían afectados unas dos horas después del turno (o 10 horas después de que el usuario inicial iniciara sesión para el primer turno).

Si va a entregar capas elásticas en un entorno basado en cambios, puede cambiar la cuenta predeterminada en la que se ejecutan todas las capas elásticas. En lugar de ejecutarse en el primer usuario que inicia sesión, puede cambiar el usuario predeterminado para todas las capas elásticas del `uLayer` servicio, que se ejecuta en la cuenta local `SYSTEM`. La cuenta `SYSTEM` corresponde a la cuenta de máquina de dominio de la máquina en la que se ejecuta el servicio `uLayer` al acceder al recurso compartido. El recurso compartido de archivos que contiene las capas elásticas requiere acceso `read-only`, ya sea para todos los usuarios o para cada cuenta de máquina.

- Para cambiar la cuenta en la que se ejecutarán capas elásticas, cree el valor de Registro `DWORD` y configúrelo en **1**:

```
HKEY_LOCAL_MACHINE\Software\Unidesk\Ulayer:AsSelfAppAttach to
1
```

- Para volver a ejecutar capas elásticas con el primer usuario que inicie sesión, establezca el valor del Registro `DWORD` en **0**:

```
HKEY_LOCAL_MACHINE\Software\Unidesk\Ulayer:AsSelfAppAttach to
0
```

- Para eliminar la configuración de modo que las capas elásticas solo se puedan ejecutar en el modo predeterminado, elimine el valor `DWORD`:

```
HKEY_LOCAL_MACHINE\Software\Unidesk\Ulayer:AsSelfAppAttach
```

## Habilitar capas elásticas en las imágenes base

Puede habilitar capas elásticas en las imágenes base (en capas) configurando la plantilla de imagen que utiliza para publicarlas:

1. En la consola de administración, seleccione la plantilla de imagen que se utilizará para publicar las imágenes en capas.
2. Seleccione la ficha **Imágenes** y, a continuación, la plantilla de imagen en la que desea habilitar las capas elásticas.
3. Seleccione **Modificar plantilla** en la barra de acciones.
4. Seleccione la ficha **Disco de imagen en capas**.
5. En el campo **Capas elásticas**, seleccione **Capas de aplicación**.
6. Seleccione la ficha Confirmar y completar y haga clic en **Guardar plantilla y publicar**.
7. Utilice el sistema de Provisioning para distribuir las máquinas virtuales.

Cuando los usuarios inician sesión, el escritorio incluye un icono para cada una de sus capas de aplicaciones elásticas.

## Ejecute el analizador de Elastic Fit en las capas

Antes de asignar una capa de aplicación de forma **elástica**, utilice **Elastic Fit Analyzer** para determinar la probabilidad de que la asignación de capas se realice correctamente.

### Análisis de Elastic Fit

En Detalles de capa, la clasificación de **ajuste elástico** indica la probabilidad de que la capa funcione cuando se asigna elásticamente.

**Buen ajuste elástico.** Esta capa funciona cuando se implementa de forma elástica.



**Ajuste elástico deficiente.** No es probable que la entrega de la capa de forma elástica funcione cuando se implementa de manera elástica. La capa puede comportarse de manera diferente que cuando se implementa en una imagen en capas.



## Detalles de ajuste elástico

Puede obtener más información sobre la clasificación de Elastic Fit de una capa de aplicación expandiendo el análisis de ajuste elástico. Si el ajuste elástico es inferior al ideal, se muestra la lista de reglas infringidas.

**Advertencia de gravedad baja.** Es improbable que la entrega de la capa de forma elástica provoque cambios en el comportamiento o la funcionalidad de la mayoría de las aplicaciones.



**Advertencia de gravedad media.** La entrega de la capa de forma elástica puede provocar cambios menores en el comportamiento o la funcionalidad de algunas aplicaciones.



**Advertencia de gravedad alta.** Es probable que la entrega de la capa de forma elástica provoque cambios significativos en el comportamiento o la funcionalidad de muchas aplicaciones.



### Nota:

Si recibe una advertencia de que se ha detectado un cambio en el archivo de clave maestra y no cambió ese archivo intencionadamente, establezca el valor del indicador `DeleteMasterKeys` de la ubicación del Registro `HKLM\System\ControlSet001\Services\Uniservice` en 1 (verdadero). Ahora, cuando se finaliza la capa de aplicaciones, los archivos de clave maestra se eliminan de la capa. Este valor no es persistente y solo funciona por revisión. Debe establecerse cada vez que se cree una revisión de la capa.

## Analizar Elastic Fit de una capa de aplicación

Todas las versiones nuevas de una versión de capa se analizan para comprobar la compatibilidad de capas elásticas cuando se finalizan. Para analizar las capas de aplicaciones existentes para Elastic Fit:

1. Inicie sesión en la consola de administración.
2. Seleccione **Capas > Capas de aplicaciones**.
3. Seleccione la capa que desea analizar y haga clic en **Analizar capa**.
4. En la ficha Seleccionar versiones, elija las Versiones de capa que quiere analizar.
5. En la ficha Confirmar y completar, haga clic en **Analizar versiones de capas**. El análisis toma segundos.
6. Para ver el **análisis de ajuste elástico**, seleccione el módulo de capas de aplicaciones, mueva el puntero del ratón sobre el icono de la capa y haga clic en el icono **Información**.

7. Expanda la **Información de la versión** para cada versión de capa y busque la calificación de Elastic Fit.
8. Para obtener un informe detallado, expanda los **detalles de ajuste elástico**. Si el ajuste elástico es inferior al ideal, se mostrará la lista de reglas infringidas.
9. Puede mostrar el árbol AD y ocultar las reglas violadas haciendo clic en un botón reconociendo que es poco probable que la capa funcione como se esperaba.

### Actualización desde versiones anteriores

Después de actualizar desde una versión anterior de App Layering, Elastic Fit Detail muestra que las versiones de capa existentes no se han analizado. Las versiones tienen un solo detalle de ajuste elástico de *alta severidad* y un ajuste elástico *deficiente*. Para obtener una lectura precisa, ejecute el análisis en las versiones de capa existentes.

### Asignar de forma elástica una capa de aplicación a usuarios y grupos de AD

La primera vez que asigne una capa de aplicaciones de forma elástica, le recomendamos que comience con una aplicación simple como **Notepad++** o **GIMP**.

1. Inicie sesión en la consola de administración como usuario administrador y seleccione **Capas > Capas de aplicaciones**.
2. Seleccione una capa de aplicación que *no vaya* a incluir en la imagen base y seleccione la versión de la aplicación que desee asignar.
3. Haga clic en **Actualizar asignaciones**.
4. Seleccione la versión de la capa de aplicaciones que desea asignar a los usuarios.
5. Omitir **asignación de plantilla de imagen**. Esto es para asignar la capa a una plantilla de imagen.
6. Seleccione los usuarios y grupos que desea que reciban esta versión de capa de aplicaciones.
7. Revise sus selecciones y haga clic en **Asignar capas**.

Cuando los usuarios inician sesión, hay un icono para cada capa elástica que se les ha asignado.

### Asignar de forma elástica una capa de aplicación a los usuarios a través de asignaciones de máquinas y asociaciones

Puede asignar capas a una máquina agregando la máquina al grupo AD o asociándola al mismo. A continuación, asigne elásticamente las capas de la aplicación al grupo AD.

Las capas asignadas a la máquina están disponibles para todos los usuarios que inicien sesión correctamente en esa máquina. El servicio App Layering busca cambios en las pertenencias y asociaciones

de grupos de AD de la máquina cada 10 minutos. Cuando los usuarios inician sesión, ven un icono para cada capa de aplicación elástica que se les ha asignado.

### Usar Active Directory para agregar el equipo al grupo de AD

Suponiendo que tiene una imagen en capas publicada arrancada en su entorno, puede agregar la máquina a un grupo AD y asignar capas elásticas al grupo AD.

1. Utilice Active Directory (AD) para agregar el equipo a un grupo de AD.
2. Seleccione una capa de aplicaciones que *no vaya* a incluir en la imagen base y asigne la capa de forma elástica a un grupo de AD.
3. Puede esperar a que AD propague los cambios y a que el servicio de App Layering, o puede forzar al servicio de App Layering a actualizar su lista de grupos de máquinas mediante *una* de las siguientes acciones:
  - Espere a que el servicio App Layering detecte los cambios (en 10 minutos de forma predefinida).
  - Reinicie el servicio App Layering.
  - Reinicie la máquina de servicio App Layering.
  - Ejecute el comando **refresh.groups** :  
C:\Archivos de programa\Unidesk\Layering Services\ulayer.exe refresh.groups

### Ejemplo

Comienza con un usuario de AD y un grupo de AD, y con una máquina que aprovisionó mediante una imagen en capas.

- Usuario de AD: *Kenia*
  - Kenya no tiene asignaciones elásticas.
- Grupo AD: *Mercadeo*
  - El grupo *Marketing* incluye al miembro Kenya.
- Máquina: *ElasticTestMachine*
  - La imagen base de *ElasticTestMachine* incluye la *capa de aplicaciones de MS Office*.

En este ejemplo, asignas de forma elástica la *capa de aplicaciones de Chrome* a *ElasticTestMachine*:

1. En AD, agrega la máquina *ElasticTestMachine* al grupo de AD de *marketing*.

2. En la consola de administración, asigna de forma elástica la *capa de aplicaciones de Chrome* al grupo de *marketing*.
3. Cuando Kenya, que forma parte del grupo Marketing, inicia sesión en *ElasticTestMachine*, recibe tanto la *capa de aplicaciones de MS Office*, que se encuentra en la imagen base, como la *capa de aplicaciones de Chrome*.
4. Cuando un usuario que *no* esté en el grupo *Marketing* inicia sesión en *ElasticTestMachine*, también recibe ambas capas: *MS Office*, porque está en la imagen base, y *Chrome*, porque *ElasticTestMachine* es miembro del grupo de *AD Marketing*.

### Administrar asignaciones elásticas

Puede hacer lo siguiente:

- Agregue una asignación elástica.
- Actualiza una capa de aplicación y asigna elásticamente la nueva versión de la capa.
- Elimine las asignaciones elásticas.
- Depure una asignación elástica.

### Actualizar una capa de aplicación y sus asignaciones elásticas

Ha agregado asignaciones elásticas a una capa de aplicación y los usuarios acceden a la aplicación como se esperaba. Se lanza una nueva versión de la aplicación, por lo que se actualiza con una nueva versión en la capa. Ahora debe asignar la nueva versión a los usuarios que tienen la capa.

1. Inicie sesión en la consola de administración y seleccione **Capas > Capas de aplicaciones**.
2. Seleccione la capa de aplicaciones asignada elásticamente que actualizó.
3. Haga clic en **Información de versión > Actualizar asignaciones**.
4. Selecciona la nueva versión.
5. *Omita* la ficha **Asignación de plantilla de imagen**.
6. En la ficha **Elastic Assignment**, hay una lista de usuarios y grupos a los que se les ha asignado una versión diferente de la capa seleccionada. Seleccione los usuarios y los grupos a los que desea asignar la nueva versión de la capa.

#### Notas:

- Si la lista es larga, use el campo **Buscar** para filtrar los resultados.
- Si la lista está vacía, haga clic en la casilla de verificación llamada **Mostrar usuarios y grupos de AD que ya están en esta versión**. Aparecerá una lista de nombres atenuados. A estos usuarios ya se les ha asignado la versión.

7. En la ficha Confirmar y completar, verifique los usuarios y grupos que desea que reciban la nueva versión.
8. Haga clic en **Actualizar asignaciones**.

### Quitar las asignaciones elásticas de una capa

1. Inicie sesión en la consola de administración y seleccione **Capas > Capas de aplicaciones**.
2. Seleccione la capa de aplicaciones para la que desea eliminar las asignaciones y seleccione **Eliminar asignaciones**.
3. Seleccione las plantillas asignadas de las que desee eliminar la capa. Se muestran las asignaciones de la capa.  
  
Si la lista es larga, use el campo Buscar para filtrar los resultados.
4. En la ficha Confirmar y completar, compruebe que las plantillas de imagen correctas están seleccionadas para recibir la nueva versión.
5. Haga clic en **Eliminar asignaciones**.

### Solución de problemas de capa elástica

Puede diagnosticar el origen de un problema de capas elásticas averiguando si la capa se está entregando y si la capa funciona correctamente. Si es necesario, recopile datos para soporte técnico, como se describe aquí.

**¿Es el problema con la entrega de capas?** ¿Son las cosas que esperaría ver cuando esta aplicación esté instalada allí?

- ¿Vaya los archivos y las entradas del registro de la capa?
- Si se supone que la aplicación está en el menú Inicio, ¿está ahí?
- Si espera que haya un acceso directo para la aplicación en el escritorio del usuario, ¿hay alguno?

Si descubre que la entrega de aplicaciones es un problema, puede recopilar los siguientes datos, abrir un caso y enviar los datos al soporte técnico.

1. Recopile los datos de estos registros:
  - Registro de eventos de aplicaciones de Windows: En el **Visor de eventos de Windows**, en **Registros de Windows**, exporte el registro de eventos de la aplicación como un archivo EVTX.
  - Registro del servicio App Layering (ulayersvc.log) —C:\ProgramData\Unidesk\Logs\ulayersvc.log



2. Recopilar los valores de estas claves del Registro:
  - HKEY\_LOCAL\_MACHINE\SOFTWARE\Unidesk\ULayer:AssignmentFile
  - HKEY\_LOCAL\_MACHINE\SOFTWARE\Unidesk\ULayer:RepositoryPath
3. Recopile el contenido de los archivos de asignación (ElasticLayerAssignments.json) y Layers (Layers.json) de la ruta del repositorio.
4. Póngase en contacto con Asistencia.

**¿Es un problema operativo?** Cualquiera de estos comportamientos puede indicar un problema de capas elásticas:

- La aplicación se está entregando pero no se inicia correctamente.
- Una operación dentro de la aplicación no funciona correctamente.
- Un problema de licencia o un problema de seguridad.
- La aplicación se inicia, pero luego se comporta mal, por ejemplo, se bloquea al iniciar o se inicia pero no funciona bien.

Si el problema con la capa es operativo, pruebe la capa de aplicación en la imagen base para descartar problemas generales de capas:

1. Agregue la capa de aplicación a una plantilla de imagen y publique una imagen en capas que incluya la capa de aplicación.
2. Inicie sesión como un usuario al que *no* se le asigne la capa de forma elástica y asegúrese de que la aplicación esté operativa en la imagen base.
3. Póngase en contacto con Asistencia con sus conclusiones.

## Implementar capas de usuarios

May 9, 2024

*Las capas de usuarios conservan las siguientes de cada usuario:*

- Configuración del perfil
- Datos
- Aplicaciones instaladas localmente en entornos VDI no persistentes

Cuando habilita capas de usuarios en una plantilla de imagen, los sistemas aprovisionados con las imágenes en capas resultantes proporcionan a cada usuario una capa de usuarios.

Cuando un usuario inicia sesión en un escritorio habilitado para capas de usuarios, se crea una nueva base de datos de índice de búsqueda. El índice incorpora información de búsqueda de la capa de

usuarios y cualquier capa elástica. La función de búsqueda solo está disponible cuando se ha completado la indexación.

En este tema se explica cómo habilitar las capas de usuarios en una plantilla de imágenes y las imágenes en capas resultantes. Los sistemas que se aprovisionan mediante las imágenes proporcionan a cada usuario una capa de usuarios.

### Tipos de capas de usuarios

Puede habilitar los siguientes tipos de capas de usuarios:

- **Completo:** Todos los datos, la configuración y las aplicaciones instaladas localmente del usuario se almacenan en su capa de usuarios.
- **Office 365:** (sistemas de escritorio) Solo los datos y la configuración de Outlook del usuario se almacenan en su capa de usuarios.
- **Sesión de Office 365:** (hosts de sesión) Solo los datos y la configuración de Outlook del usuario se almacenan en su capa de usuarios.

Puede habilitar una capa de usuarios completa, una capa de usuarios de Office 365 o una capa de usuarios de Session Office 365. La capa de usuario completa incluye todo lo que guarda la capa de usuarios de Office 365/Sesión de Office 365, junto con la configuración y los datos de otras aplicaciones.

#### Nota:

Office 365 y Session Office 365 están en desuso.

### Requisitos

Antes de habilitar las capas de usuarios, asegúrese de cumplir los requisitos que se aplican a los siguientes tipos de capas de usuarios:

- Todos los tipos de capas de usuarios
- Capas de usuarios completas
- Capas de usuarios de Office 365 y sesión de Office 365

### Todas las capas de usuarios

Para habilitar las capas de usuarios necesita:

- Ancho de banda de red adecuado. El ancho de banda y la latencia tienen un efecto significativo en la capa de usuarios. Cada escritura va a través de la red.

- Suficiente espacio de almacenamiento asignado para los datos de los usuarios, los ajustes de configuración y las aplicaciones instaladas localmente. (El dispositivo utiliza la ubicación de almacenamiento principal para empaquetar capas, publicar imágenes en capas y publicar capas elásticas).

### Capas de usuarios completas

- Al usar Profile Management con una capa de usuario completa, debe borrar la eliminación de la información del usuario al cerrar la sesión. Según cómo esté implementando la configuración, puede borrar la eliminación mediante una de las siguientes opciones:
  - Objeto de directiva de grupo.
  - La directiva del Delivery Controller (DDC).

### Capas de usuarios de Office 365 y sesión de Office 365

- Utilice un gestor de perfiles, como Citrix Profile Manager. De lo contrario, Outlook asume que cada usuario que inicia sesión es un usuario nuevo y crea archivos del sistema operativo para ellos.
- La capa de Office debe incluirse en la plantilla de imagen e implementarse en la imagen en capas. Sin embargo, puede utilizar otras capas elásticas con una capa de usuarios de Office 365.
- Microsoft Office solo se admite como capa de aplicaciones en una imagen publicada, no como capa elástica.
- Los cambios en la ubicación predeterminada de los archivos de índice de búsqueda *no* se conservan en la capa de Office 365.
- Esta función se ha probado para un escritorio por usuario a la vez (Single Sign-On).

#### Nota:

Office 365 y Session Office 365 están en desuso.

### Compatibilidad

Las capas de usuarios completas se admiten en las siguientes plataformas:

- **Sistemas operativos:**  
todos los sistemas operativos deben configurarse en modo de usuario único para que funcionen con capas de usuarios. Los servidores no se pueden usar en modo multiusuario. No se admiten las capas de usuarios en los hosts de sesión.

- Windows 10, 64 bits
  - Windows 11, 64 bits (solo si se implementa en una plataforma habilitada para la composición de descarga)
  - Windows Server 2016, solo modo de usuario único
  - Windows Server 2019, solo modo de usuario único
- **Plataformas de publicación:**  
las capas de usuarios se admiten en las siguientes plataformas de publicación.
    - Citrix Virtual Desktops

### Aplicaciones que *no se admiten en una capa de usuarios*

Las siguientes aplicaciones no se admiten en la capa de usuarios. *No instale estas aplicaciones de forma local:*

- Aplicaciones empresariales: las aplicaciones empresariales, como MS Office y Visual Studio, deben instalarse en capas de aplicaciones. Las capas de usuarios se basan en la misma tecnología que las capas elásticas. Al igual que con las capas elásticas, nunca use capas de usuarios para estas aplicaciones empresariales.
- Aplicaciones con controladores que utilizan el almacén de controladores. Ejemplo: un controlador de impresora.

#### **Nota:**

Puede hacer que las impresoras estén disponibles mediante las directivas de grupo. Consulte Impresoras instaladas por GPO-en la siguiente sección.

- Aplicaciones que modifican el hardware o la pila de red. Ejemplo: un cliente VPN.
- Aplicaciones que tienen controladores de nivel de arranque. Ejemplo: un antivirus.
- Aplicaciones que requieren agregar un usuario o grupo local. Los usuarios y grupos locales que agregue como parte de la instalación de una aplicación solo persisten en la capa del sistema operativo. Considere la posibilidad de instalar una aplicación en una capa que se incluirá en la imagen base, con el usuario o administrador necesario agregado a la capa de sistema operativo.

### Actualizaciones de Windows

Las actualizaciones de Windows deben estar inhabilitadas en la capa de usuarios.

## Complementos de almacén de Outlook

Citrix Profile Management inhabilita los complementos de almacenamiento.

La primera vez que se inicia Outlook, el icono de **Tienda/complementos** de la cinta muestra una ventana con una larga lista de complementos. Durante el inicio de sesión inicial, si instala complementos, aparecerán en la cinta de opciones en los inicios de sesión posteriores. Si no instala los complementos, el icono **Store/Add-ins** muestra una ventana blanca vacía.

## Impresoras instaladas por GPO-

Para los usuarios de escritorios no persistentes que ejecutan Windows 10, puede instalar impresoras mediante una directiva de grupo. Con una directiva implementada, las impresoras aparecen en Dispositivos e impresoras de los usuarios, en la configuración de la impresora de aplicaciones y en el Administrador de dispositivos.

Para configurar impresoras instaladas en GPO-GP:

1. Habilite las capas de usuarios en la plantilla de imagen.
2. Asegúrese de que el escritorio esté unido al dominio (en la capa Plataforma).
3. Cree una directiva de grupo para implementar cada impresora de red y asígnala a la máquina.
4. Cuando haya iniciado sesión como usuario de dominio, compruebe que la impresora aparece en Dispositivos e impresoras, Bloc de notas y Administrador de dispositivos.

## Formato de capa de usuario

Los discos virtuales de capa de usuarios se crean con el formato VHDX. Puede seguir utilizando los archivos VHD de la capa de usuarios existentes sin convertirlos ni volver a crearlos. Sin embargo, cuando los archivos VHD y VHDX existen en la misma carpeta, el archivo VHDX tiene prioridad.

## Cómo anular el formato VHDX para la creación de discos virtuales de capa de usuarios

Puede cambiar el comportamiento para obligar a las capas de usuarios que se crean a utilizar el formato VHD. Para anular este comportamiento, utilice el siguiente parámetro del registro del sistema:

- Ruta: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ulayer`
- Nombre: `DefaultUserLayerVHDXDisabled`
- Tipo: `DWORD`
- Datos: `1`

## Recuperación de espacio de capa de usuarios/UPL

Puede usar la función de **recuperación de espacio de capa de usuarios/UPL** para optimizar automáticamente los archivos VHDX cada vez que el usuario cierre sesión.

### Cómo habilitar la recuperación de espacio de capa de usuarios/UPL

Antes de habilitar la **recuperación de espacio de capa de usuarios/UPL**:

- El servicio de optimización de unidades `defragsvc` debe estar habilitado y en ejecución. Este servicio está inhabilitado para las capas de sistema operativo existentes.
- Citrix recomienda crear una nueva versión de la capa de sistema operativo antes de habilitar la función.

Puede habilitar la **recuperación de espacio de capa de usuarios/UPL** de cualquiera de las siguientes maneras:

- Uso de Citrix Studio
- Uso del Editor del Registro de Windows
  - Ruta: `HKLM\SOFTWARE\Policies\Citrix\UserPersonalizationLayerConfig`
  - Nombre: `UserLayerCompactionEnabled`
  - Tipo: `DWORD`
  - Datos: 1 (Valor predeterminado: 0)

Esta función está inhabilitada de forma predeterminada.

## Habilitar capas de usuarios en una imagen en capas

Para implementar capas de usuarios, habilite las capas mediante la configuración de una plantilla de imagen. Para obtener pasos detallados, consulte [Crear o clonar una plantilla de imagen](#). El resto de este artículo proporciona detalles sobre el tamaño, el almacenamiento, la configuración de la seguridad, el movimiento y la reparación de capas de usuarios. También cubre los pasos para personalizar las notificaciones para los usuarios finales.

## Ubicación de la capa de usuarios

Cuando una plantilla de imagen tiene las capas de usuarios habilitadas, las imágenes que publique conservan los datos, la configuración y las aplicaciones instaladas localmente de los usuarios.

Cuando las capas de usuarios están habilitadas, debe agregar ubicaciones de almacenamiento para las capas.

### **Importante:**

No permita que las capas de usuarios se guarden en el recurso compartido de archivos principal del dispositivo. De lo contrario, se puede agotar el espacio para:

- Actualizando el software.
- Servir capas elásticas a los usuarios.
- Guardar los archivos que está moviendo a un hipervisor para el que no hay ningún conector compatible.

La primera ubicación de almacenamiento agregada al dispositivo se convierte en la ubicación predeterminada para las capas de usuarios que no están asociadas a ninguna otra ubicación de almacenamiento. Cuando agrega más ubicaciones de almacenamiento, se muestran en orden de prioridad.

Puede asignar grupos de usuarios a cada ubicación de almacenamiento que agregue.

### **Donde se almacena una capa de usuarios cuando el usuario pertenece a más de un grupo**

Si un usuario pertenece a más de un grupo y esos grupos se asignan a diferentes ubicaciones de almacenamiento, la capa de usuarios de la persona se almacena en la ubicación de almacenamiento de máxima prioridad.

Si cambia el orden de prioridad de las ubicaciones de almacenamiento a las que se asigna el usuario *después* de guardar la capa de usuarios de la persona en la ubicación de mayor prioridad, los datos guardados hasta ese punto permanecen en la ubicación original. Para conservar la capa de usuarios de la persona, *debe* copiar su capa de usuarios en la nueva ubicación de mayor prioridad.

### **Cómo especificar la ubicación del recurso compartido de archivos de capa de usuarios en una imagen específica**

Puede admitir a un usuario que necesite acceder a dos imágenes separadas al mismo tiempo, donde ambas imágenes:

- Necesita la persistencia de las capas de usuarios.
- Se crearon mediante la misma capa de SO.

Para configurar asignaciones de recursos compartidos de archivos de capa de usuarios:

1. Agregue la siguiente clave de registro en una o más de sus imágenes publicadas *antes de que* cualquier usuario inicie sesión:

```
[HKLM\Software\Unidesk\ULayer]
"UserLayerSharePath"
```

Puede agregar la clave anterior a la capa de plataforma, a una capa de aplicación o como directiva de grupo de máquinas.

Si agrega la clave **UserLayerSharePath** a la imagen antes de que un usuario inicie sesión, el dispositivo ignora las asignaciones de recursos compartidos de capa de usuarios. En su lugar, todos los usuarios de la máquina utilizan el recurso compartido especificado para los VHDX o VHD de la capa de usuarios. El subárbol `\Users` se anexa a esta clave para localizar las capas reales.

### Cómo especificar una ruta de acceso de capa de usuarios personalizada

Puede establecer una ruta personalizada creando un valor `REG_SZ` llamado `CustomUserLayerPath` en la clave `HKLM\Software\Unidesk\Ulayer`. La clave `HKLM\Software\Unidesk\Ulayer` puede incluir variables de entorno y atributos de Active Directory (AD).

En el valor `CustomUserLayerPath`, todas las variables del sistema se pueden expandir, pero las únicas variables de usuario que se pueden expandir son `%USERNAME%` y `%USERDOMAIN%`. La ruta completa es:

```
<CustomUserLayerPath>\<OSID_OSNAME>
```

Si establece la ruta de capa de usuarios personalizada mediante GPO, utilice `%<USERNAME>%` y `%<USERDOMAIN>%` para evitar que el GPO expanda las rutas.

- Si `CustomUserLayerPath` está definido, se usa en lugar de cualquier otra ruta.
- Si `CustomUserLayerPath` no está definido, se usa `UserLayerSharePath`, que está dentro de la misma clave.
- Si `UserLayerSharePath` no está definido, se utiliza la `StorageLocation` que aparece en el JSON para el dispositivo App Layering. Puede modificar la `UserLayerSharePath` en la consola de administración, en la configuración **Sistema > Ubicación de almacenamiento de la capa de usuarios**.
- Si no hay ninguna `StorageLocation` enumerada en el JSON del dispositivo App Layering, se usa `RepositoryPath`. Puede modificar la `RepositoryPath` en la misma ubicación de registro que `CustomUserLayerPath` y `UserLayerSharePath`.
- Cuando `CustomUserLayerPath` se define, la ruta en la que se crean las capas de usuarios es la ruta expandida, más `\<OSID_OSNAME>`. Todas las demás rutas son rutas compartidas y se anexan a `\Users\<Domain_UserName>\<OSID_OSNAME>`.

Si usa atributos de AD, los atributos deben estar encerrados en hashes (por ejemplo, `#aMAccountName#`). Los atributos de AD personalizados se pueden usar para definir variables organizativas, como ubicaciones o usuarios. Los atributos distinguen mayúsculas y minúsculas.

Ejemplos:

- `\\server\share\\#sMAccountName#` almacena la configuración del usuario en la ruta UNC



- `\\server\share\JohnSmith` (si `#sAMAccountName#` se resuelve en JohnSmith para el usuario actual)

### Dónde se crean capas de usuarios en el dispositivo

En el recurso compartido de archivos de red del dispositivo, las capas de usuarios se crean en la carpeta **Usuarios**. Por ejemplo:

```
1 \MyServer*MyShare*\Users
2 <!--NeedCopy-->
```

Cada usuario tiene su directorio dentro del directorio de usuarios. El directorio de un usuario se denomina de la siguiente manera:

```
1 Users*DomainName_username**OS-Layer-ID-in-hex**OS-Layer-name**
 username*.vhd
2 <!--NeedCopy-->
```

Por ejemplo:

- Nombre de inicio de sesión del usuario: **jdoue**
- Dominio del usuario: **testdomain1**
- Capa de sistema operativo: MyOSLayer (el ID está en formato hexadecimal: 123456)
- La capa de usuarios se crea en:

```
1 \MyServer\MyShare\Users\testdomain1_jdoue\123456_MyOSLayer\jdoue.vhd
2 <!--NeedCopy-->
```

### Dónde los usuarios pueden acceder a su capa de usuarios

Cuando se crean capas de usuarios completas, los usuarios pueden acceder a todo C:\ (sujeto a los derechos de Windows y a la seguridad de la empresa en los directorios).

Cuando se crean capas de Office 365, el directorio de capas de usuarios se redirige a la capa de Office 365:

```
1 C:\user\<username\>\Appdata\local\Microsoft\Outlook
2 <!--NeedCopy-->
```

### Agregar una ubicación de almacenamiento

Para agregar una ubicación de almacenamiento para las capas de usuarios de una imagen:

1. Inicie sesión en la consola de administración.

2. Seleccione **Sistema > Ubicaciones de almacenamiento de la capa de usuarios**. Se muestra una lista de recursos compartidos de archivos, excepto el recurso compartido de archivos principal del dispositivo.
3. Seleccione **Agregar ubicación de almacenamiento** e introduzca un **nombre** y una **ruta de red** para la nueva ubicación.
4. En **Asignaciones**, haga clic en **Agregar grupos**.
5. Expanda el directorio, seleccione los usuarios que desee y haga clic en **Guardar**.
6. Haga clic en **Confirmar y completar** para agregar la ubicación de almacenamiento.

Una vez que se agregan las ubicaciones de almacenamiento, debe establecer la seguridad en las carpetas de capa de usuarios.

### Configurar la configuración de seguridad en las carpetas de capa de usuarios

Puede especificar más de una ubicación de almacenamiento para las capas de usuarios. Para cada ubicación de almacenamiento (incluida la ubicación predeterminada), debe crear una subcarpeta `\Users` y proteger esa ubicación.

Un administrador de dominio debe establecer la seguridad de cada carpeta de capa de usuarios en los siguientes valores:

| Nombre del parámetro                                               | Valor                                                                                                                | Aplicar a                                     |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Propietario creador                                                | Modificar/eliminar subcarpetas y archivos*                                                                           | Subcarpetas y archivos únicamente             |
| Derechos de propietario                                            | Modificar                                                                                                            | Subcarpetas y archivos únicamente             |
| Usuarios o grupos                                                  | Crear carpeta/anexar datos; Atravesar carpeta/ejecutar archivo; Mostrar lista de carpetas/leer datos; Leer atributos | Solo carpeta seleccionada                     |
| Sistema                                                            | Control total                                                                                                        | Carpeta, subcarpetas y archivos seleccionados |
| Administradores de dominio y grupo de administradores seleccionado | Control total                                                                                                        | Carpeta, subcarpetas y archivos seleccionados |

\*En algunos servidores, **Creator Owner** requiere **Eliminar subcarpetas y archivos** (un permiso avanzado) para que App Layering pueda limpiarse después de reparar la capa de usuarios.

Para configurar la seguridad en las carpetas de capa de usuarios:

1. Inicie sesión en la consola de administración.
2. Haga clic en **Sistema > Ubicaciones de almacenamiento de capa de usuarios** Los recursos compartidos de archivos mostrados son las ubicaciones de almacenamiento definidas para las capas de usuarios. Supongamos que ha definido tres ubicaciones de almacenamiento para poder administrar el almacenamiento del Grupo 1 y el Grupo 2 por separado del resto de la organización:

- *Default location* - \ MyDefaultShare\ UserLayerFolder\
  - *Group1* - \\MyGroup1\Share\UserLayerFolder\
    - *Group2* - \\MyGroup2\Share\UserLayerFolder\

**Note:** The appliance's main file share, which is used for storing OS, app, and platform layers, is *not* listed as a user layer storage location. For more about the App Layering file share, see [Setting up a file share](#).

3. Cree un subdirectorio `\Users` en cada recurso compartido de archivos:

```
1 \MyDefaultShare\UserLayerFolder\Users\
2
3 \MyGroup1Share\UserLayerFolder\Users\
4
5 \MyGroup2Share\UserLayerFolder\Users\
6 <!--NeedCopy-->
```

1. Aplique la lista anterior de configuraciones de seguridad a cada subdirectorio en `\Users`.

## Aplicar directivas de Studio de capa de personalización de usuario a capas de usuarios

Cuando las capas de usuarios están habilitadas en una imagen en capas, puede anular la ruta y el tamaño de capa predeterminados del repositorio para las capas de usuarios mediante la configuración de las directivas de Citrix Studio correspondientes:

- **Ruta del repositorio de capas de usuarios:** define el lugar de la red para acceder a las capas de usuarios.
- **Tamaño de la capa de usuarios en GB:** define el tamaño para permitir el crecimiento de los discos de la capa de usuarios.

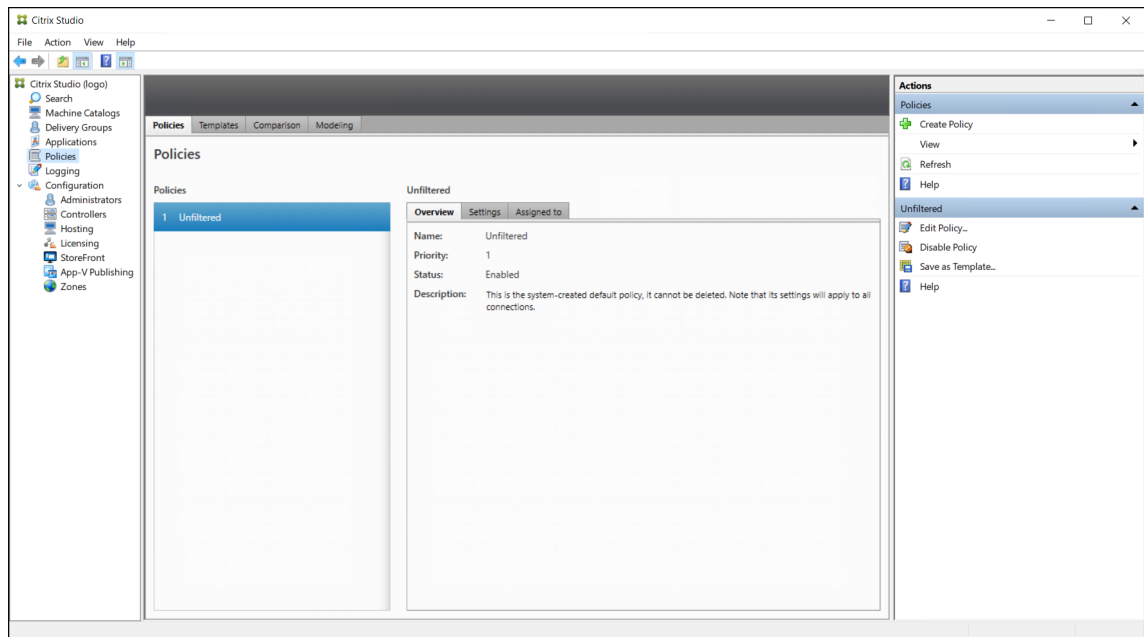
Si la imagen publicada ejecuta una versión compatible del VDA y se han definido estas directivas, la ruta de acceso y el tamaño definidos en las directivas tendrán la máxima prioridad.

La próxima vez que el usuario inicie sesión tendrá efecto un aumento en el tamaño de la capa de usuarios asignado. La disminución del tamaño de la capa de usuarios asignada no afecta a las capas de usuarios existentes.

### Definir las directivas de Studio para las capas de usuarios de una imagen

Para configurar las directivas de Citrix Studio para las capas de usuarios de una imagen en capas:

1. En Citrix Studio, seleccione **Directivas** en el panel de navegación:



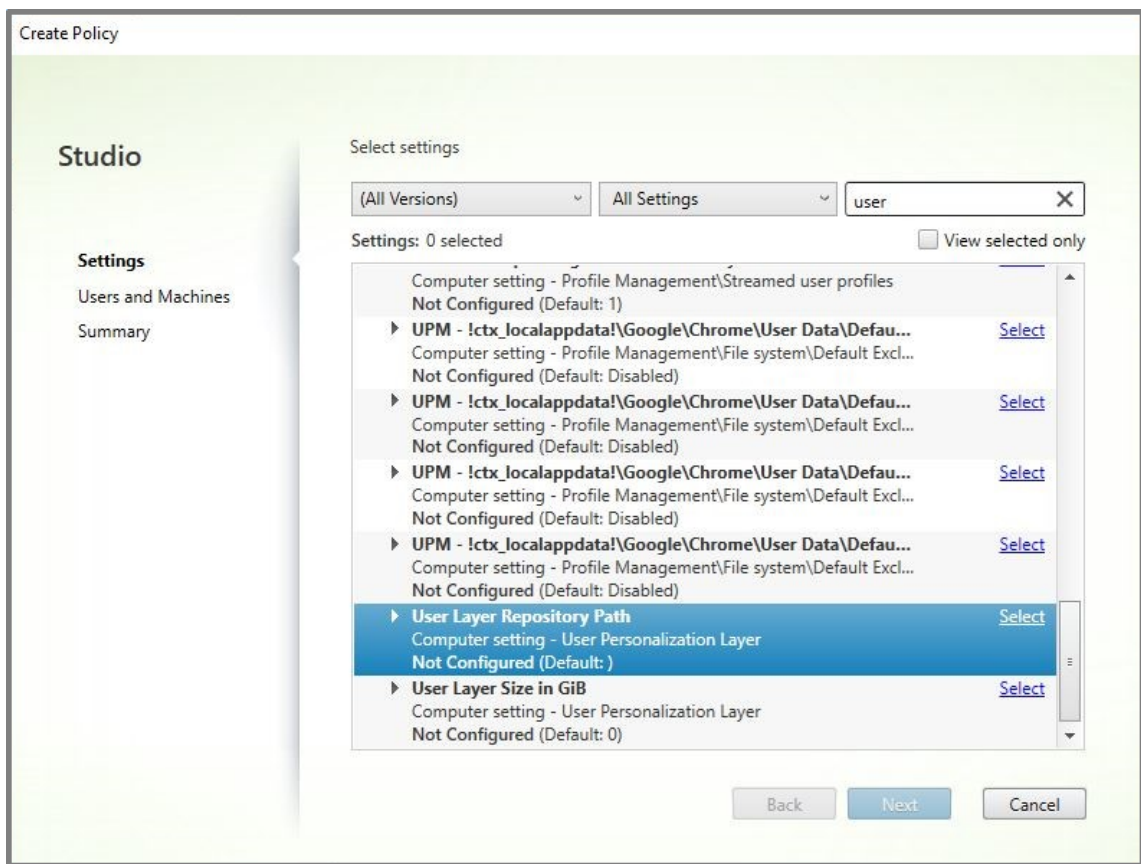
2. Seleccione **Crear directiva** en el panel Acciones. Aparecerá la ventana Crear directiva.
3. Escriba “capa de usuarios” en el campo de búsqueda. En la lista de directivas disponibles, aparecen las dos directivas siguientes:

- Ruta del repositorio de capas de usuarios
- Tamaño de capa de usuarios en GB

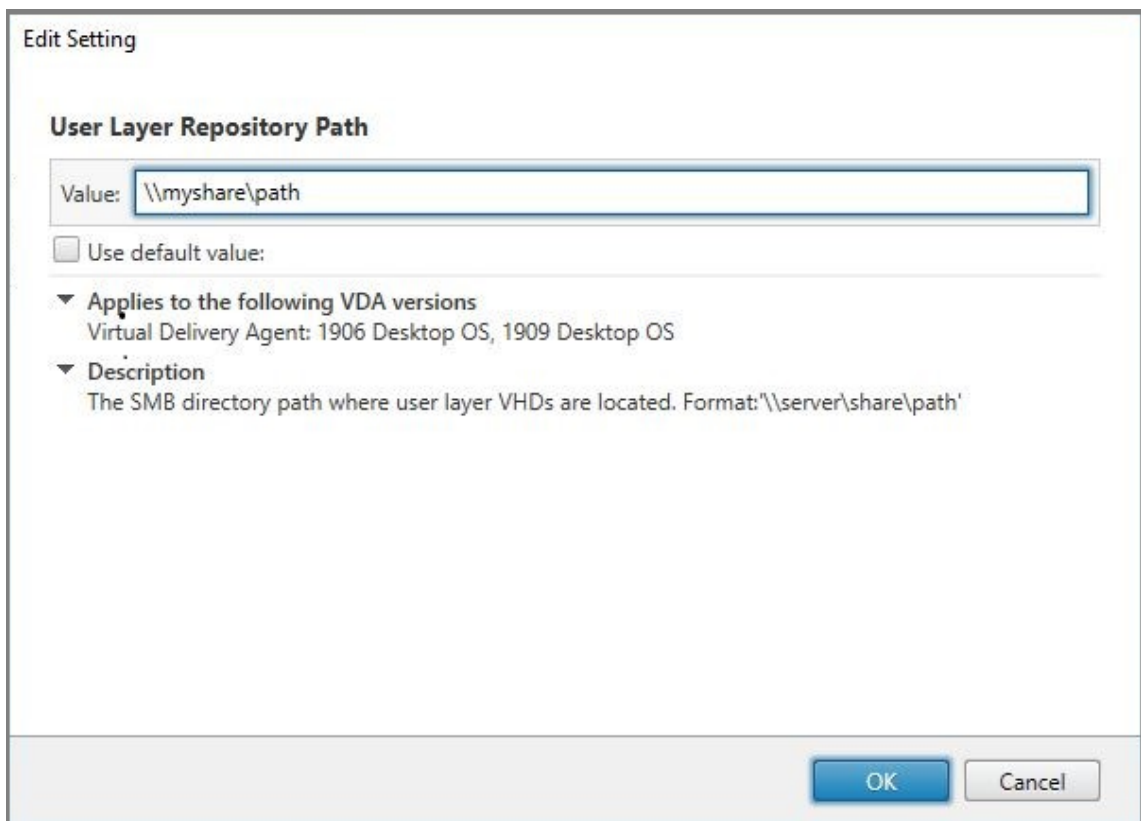
#### **Nota:**

La próxima vez que el usuario inicie sesión tendrá efecto un aumento en el tamaño de la capa de usuarios asignado. Una disminución del tamaño de capa de usuarios asignado no afecta a las capas de usuarios existentes.

4. Haga clic en **Seleccionar** junto a **Ruta del repositorio de capas de usuarios**. Se muestra la ventana Modificar parámetro .



5. Introduzca una ruta en el formato `\\server name or address\folder name` del campo **Valor**, haga clic en **Aceptar**:



6. Opcional: haga clic en **Seleccionar** junto a Tamaño de capa de usuarios en GB:

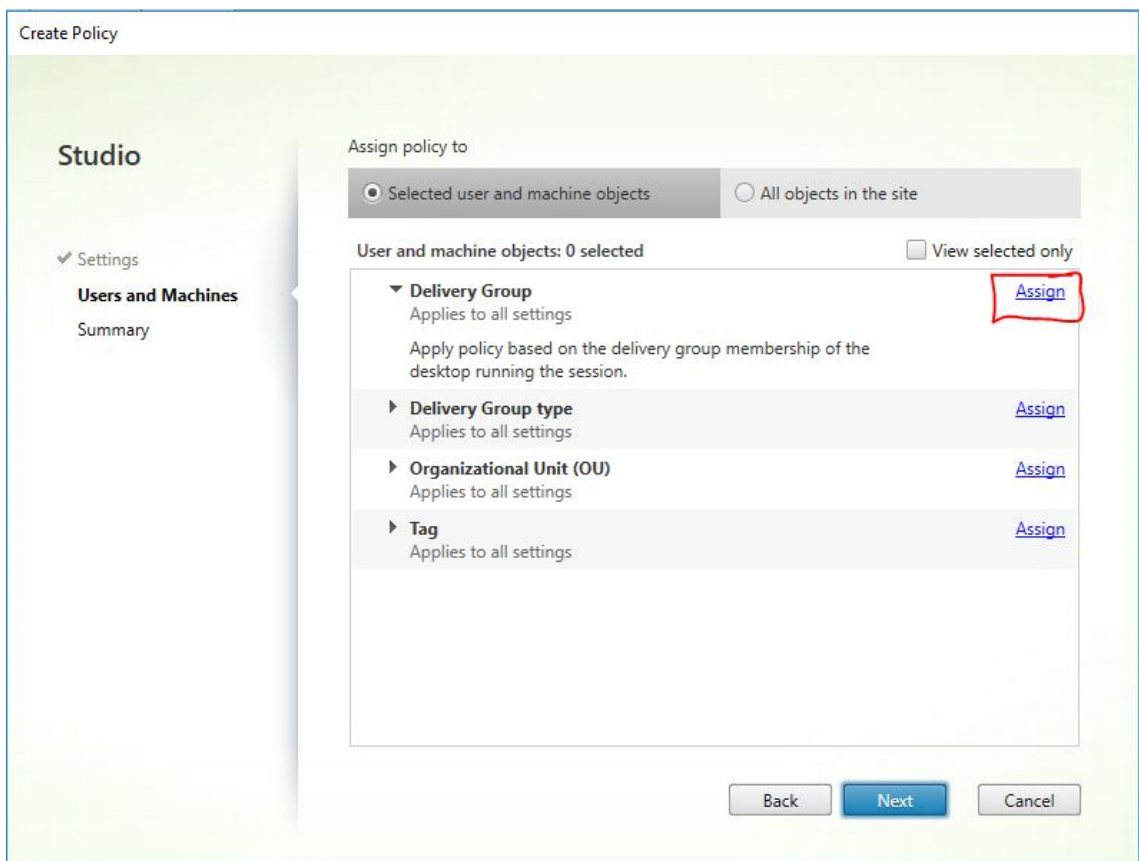


7. Aparece la ventana **Modificar configuración**.
8. Opcional: cambie el valor predeterminado de **'0'** al **tamaño máximo (en GB)** que la capa de usuarios puede aumentar. Haga clic en **Aceptar**.

**Nota:**

Si mantiene el valor predeterminado, el tamaño máximo de las capas de usuarios es de 10 GB.

9. Haga clic en **Siguiente** para configurar Usuarios y máquinas. Haga clic en el enlace **Asignar grupo de entrega** resaltado en esta imagen:



10. En el menú Grupo de entrega, seleccione el grupo de entrega creado en la sección anterior. Haga clic en Aceptar.



Assign Policy

**Delivery Group**

**Applies to:** Virtual Delivery Agent: 5.6, 7.0 Server OS, 7.0 Desktop OS, 7.1 Server OS, 7.1 Desktop OS, 7.5 Server OS, 7.5 Desktop OS, 7.6 Server OS, 7.6 Desktop OS, 7.7 Server OS, 7.7 Desktop OS, 7.8 Server OS, 7.8 Desktop OS, 7.9 Server OS, 7.9 Desktop OS, 7.11 Server OS, 7.11 Desktop OS, 7.12 Server OS, 7.12 Desktop OS, 7.13 Server OS, 7.13 Desktop OS, 7.14 Server OS, 7.14 Desktop OS, 7.15 Server OS, 7.15 Desktop OS, 7.16 Server OS, 7.16 Desktop OS, 7.17 Server OS, 7.17 Desktop OS, 7.18 Server OS, 7.18 Desktop OS, 1808 Server OS, 1808 Desktop OS, 1811 Server OS, 1811 Desktop OS, 1903 Server OS, 1903 Desktop OS, 1906 Server OS, 1906 Desktop OS, 1909 Server OS, 1909 Desktop OS

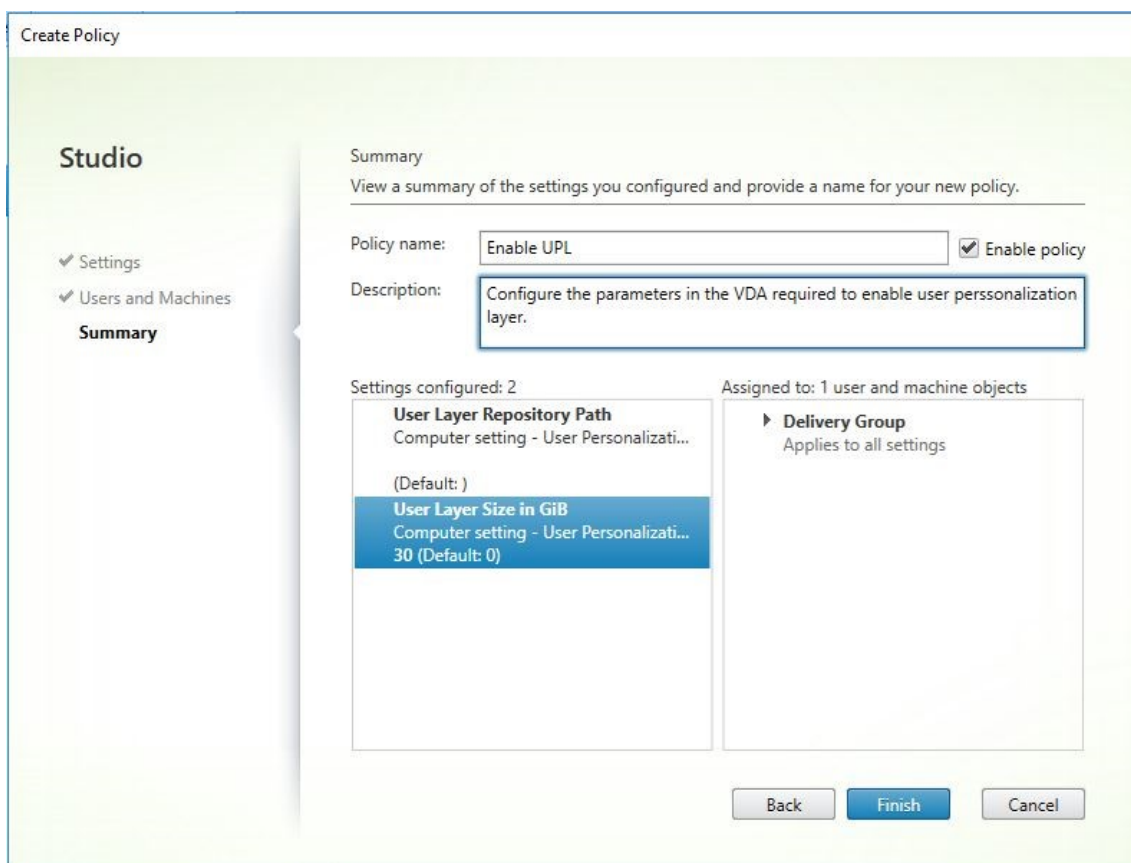
Apply policy based on the delivery group membership of the desktop running the session.

**Delivery Group elements:**

| Mode                                       | Controller | Delivery Group |     |
|--------------------------------------------|------------|----------------|-----|
| Allow                                      |            | Win10 - UPL    | + - |
| <input checked="" type="checkbox"/> Enable |            |                |     |

OK Cancel

11. Introduzca un nombre para la directiva. Haga clic en la casilla de verificación para habilitar la política y, a continuación, haga clic en **Finalizar**.



## Mover capas de usuarios existentes a una nueva ubicación de almacenamiento

Copie cada ubicación de almacenamiento de capas de usuarios en su nueva ubicación:

1. Asegúrese de que la capa de usuarios no está en uso.

Si un usuario inicia sesión antes de mover su capa de usuarios, se crea una nueva capa de usuarios. No se pierden datos, pero si sucede, asegúrese de:

- Mueva la capa de usuarios recién creada al nuevo directorio.
- Conservar las ACL del usuario.

2. Navegue hasta el directorio que contiene el archivo VHDX o VHD de la capa de usuarios.
3. Con el siguiente comando, copie cada uno de los archivos VHDX o VHD de la capa de usuario de la ubicación anterior a la nueva.

```
1 xcopy Domain1\User1 Domain1_User1\ /O /X /E /H /K
2 <!--NeedCopy-->
```

1. Compruebe que todos los permisos son correctos en los siguientes directorios y archivos dentro de ellos:

```
1 \\Root\Engineering\Users
2
3 \\Root\Engineering\Users\Domain1_User1\...
4
5 \\Root\Engineering\Users\Domain2_User2\...
6 <!--NeedCopy-->
```

### Si permite a los usuarios crear capas de usuarios

Si decide permitir que los usuarios creen capas de usuarios, debe limpiar manualmente los directorios y archivos originales de su recurso compartido.

### Tamaño de capa de usuarios

De forma predeterminada, el espacio en disco permitido para las capas de usuarios de una imagen es de 10 GB por capa.

Puede cambiar el tamaño predeterminado de la capa de usuarios mediante:

- Definición de una cuota para el recurso compartido de capa de usuarios
- Configuración de una anulación del Registro

Cuando se utilizan capas de usuarios de Office 365, la capa de Outlook tiene un valor predeterminado de 10 GB, pero Outlook establece el tamaño del volumen en función de la cantidad de espacio libre en disco. Outlook utiliza más o menos espacio en función de lo que está disponible en la imagen en capas. El tamaño notificado se basa en la imagen en capas.

### Orden de precedencia

Al implementar capas de usuarios, el dispositivo utiliza el siguiente orden de prioridad para determinar el tamaño de la capa de usuarios:

- Cuota de disco en el tamaño de capa de usuarios establecida mediante:
  - Administrador de recursos de servidor de archivos de Microsoft (FSRM)
  - Administrador de cuotas de Microsoft
- Anulación del registro para los discos de capa de usuarios:  
(HKLM\SOFTWARE\Unidesk\ULayer\DefaultUserLayerSizeInGb)
- Tamaño predeterminado de la capa de usuarios (10 GB)

## Cambiar el tamaño de la capa de usuarios

El aumento al tamaño asignado de la capa de usuarios tendrá efecto la próxima vez que el usuario inicie sesión. Reducir al tamaño de capa de usuario asignado no afecta a las capas de usuarios existentes.

## Definir una cuota de disco para discos de capa de usuarios

Puede establecer una cuota fija en el tamaño del disco de la capa de usuarios mediante cualquiera de las herramientas de cuota de Microsoft:

- Administrador de recursos del servidor de archivos (FSRM)
- Administrador de cuotas

La cuota debe establecerse en el directorio de capas de usuarios, denominado **Usuarios**.

### Nota:

Cambiar la cuota (aumentando o disminuyendo) solo afecta a las nuevas capas de usuarios. El tamaño máximo de las capas de usuarios existentes se estableció previamente y permanece sin cambios cuando se actualiza la cuota.

## Establecer anulaciones de registro de tamaño máximo

Puede anular el tamaño máximo predeterminado de la capa de usuarios mediante el registro de las máquinas administradas. Las siguientes claves del Registro son opcionales. No es necesario configurar estas claves para el funcionamiento normal. Si necesitas una de estas claves, agréguela manualmente mediante una capa o un GPO/GPP.

Raíz del Registro: HKLM\Software\Unidesk\Ulayer

| Clave                        | Tipo   | Valor predeterminado    | Descripción                                                                                                             |
|------------------------------|--------|-------------------------|-------------------------------------------------------------------------------------------------------------------------|
| UseQuotaIfAvailable          | Cadena | True; False             | True para habilitar la detección y el uso de cuotas. False para inhabilitar.                                            |
| DefaultUserLayerSizeInGBWord |        | Definido por el usuario | El tamaño de la capa de usuarios en GB (por ejemplo, 5, 10, 23,...) Si no se especifica, el valor predeterminado es 10. |

| Clave             | Tipo  | Valor predeterminado    | Descripción                                                                                                                                                                                                                                                                    |
|-------------------|-------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| QuotaQuerySleepMS | DWord | Definido por el usuario | Número de milisegundos que se debe esperar después de crear el directorio para la capa de usuarios antes de comprobar si tiene una cuota. Algunos sistemas de cuota tardan tiempo en aplicar la cuota al nuevo directorio, por ejemplo, FSRM. La cuota predeterminada es 1000. |

---

## Reparar una capa de usuarios

La función de reparación de capas de usuarios permite eliminar una aplicación y sus archivos de la capa de usuarios de una persona. Puede usar esta función después de entregar una aplicación a los usuarios que ya la hayan instalado localmente en su capa de usuarios. La función de reparación elimina los archivos en conflicto, ya sea que entregue la nueva capa de aplicación como parte de la imagen base o como capa elástica.

- **Ejemplo 1:** Crea una capa de aplicación que incluye el archivo, you.txt, y proporciona la capa de aplicación de forma elástica a los usuarios. Cuando un usuario cambia el archivo, los cambios se almacenan en su capa de usuarios. Si sus cambios rompen la aplicación o si el archivo está dañado, la función de reparación de la capa de usuarios le permite limpiar el archivo problemático quitándolo de la capa de usuarios. A continuación, el usuario ve el archivo que se proporciona de forma elástica como parte de la capa de aplicación.
- **Ejemplo 2:** Un usuario elimina una aplicación que se le ha asignado de forma elástica. Como la capa de usuarios tiene prioridad, una vez que se elimina la copia local de la aplicación del usuario, el usuario ya no ve esa versión de la aplicación. El usuario ve la capa de aplicaciones que está asignada como capa elástica.
- **Ejemplo 3:** Un usuario instala una aplicación localmente y, más adelante, el administrador crea una capa de aplicaciones para la misma aplicación. La función de reparación de capa de usuarios elimina los archivos conflictivos instalados por la aplicación de la capa de usuarios para que

el usuario consulte la versión suministrada en la capa de aplicación.

### Cómo funciona la reparación de capas de usuarios

El dispositivo genera archivos JSON de reparación de capas de usuarios que puede utilizar para limpiar o restaurar la capa de usuarios. Copie manualmente los archivos JSON en las capas de usuarios que necesitan la reparación.

Si las carpetas de carga de reparación no existen en el recurso compartido de red, se crean automáticamente. El dispositivo escribe los archivos JSON de reparación en los siguientes directorios en el recurso compartido de archivos:

```
1 <StorageLocationShare>\Unidesk\Layers\App\Repair\
2 <StorageLocationShare>\Unidesk\Layers\App\PackageAppRules
3 <!--NeedCopy-->
```

El directorio de **reparación** contiene los archivos JSON de cada versión de cada capa que conoce el dispositivo. Cada vez que finaliza una nueva capa de aplicación o una versión de la misma, el dispositivo genera y carga los archivos de reparación.

Los archivos de reparación de cada capa incluyen:

```
1 UserLayerRepair_LayerIdInDecimal_RevisionIdInDecimal.json
2 UserLayerRepair_<layer id>_<layer version>.json
3 <!--NeedCopy-->
```

Para ver el ID de capa en la consola, haga clic en la ficha **Capa**, seleccione la capa y haga clic en el icono **i**. El ID de capa se muestra junto con otros detalles de capa.

El directorio **PackageAppRules** contiene las reglas de aplicación de paquetes para cada versión de una capa de usuarios.

### ¿Cuánto tiempo se tarda en reparar una capa?

El tiempo del proceso de reparación varía en función del tamaño de la capa y del número de objetos que se deben eliminar.

Una reparación de una capa que necesita ser montada pero que no tiene operaciones reales que realizar agrega unos 5 segundos al proceso de inicio de sesión. El tiempo de inicio de sesión se reduce a 2 segundos cuando la capa de aplicación se incluye en la imagen.

El tiempo varía dependiendo de las operaciones. Para una capa de aplicación típica, es menos de 10 segundos, por lo que de 12 a 15 en total.

## Reparar una capa de usuarios

Para reparar la capa de usuarios de un usuario:

1. Identifique la versión de una capa de aplicación que debe repararse.
2. Busque los archivos **UserLayerRepair** generados previamente. Si los archivos no se han generado, póngase en contacto con el Soporte de App Layering. El ingeniero de soporte técnico puede generar los archivos de reparación manualmente para usted.
3. Copie los archivos de reparación de la capa de usuarios directamente en la ubicación del VHDX o VHD del usuario. La próxima vez que el usuario inicie sesión, se realizará una operación de reparación.

Si se completa la tarea de reparación de la capa de usuarios, se quita el archivo `UserLayerRepair.JSON`.

### Nota:

Si existe un archivo de reglas JSON en el recurso compartido y el usuario lo ha modificado, no se sobrescribe. Esto permite a los usuarios modificar esos archivos según lo deseen.

## Archivos de registro para reparaciones de capas de usuarios

El archivo de registro, `ulayersvc.log`, contiene la salida del ejecutable de reparación de capa de usuarios.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

Todos los cambios realizados durante la limpieza se registran allí, junto con cualquier otro cambio que el servicio registra.

## ¿Qué sucede si falla una reparación?

En caso de fallo, el usuario recibe un mensaje en el que se indica que la reparación ha fallado y que debe ponerse en contacto con su administrador. Puede configurar el mensaje en el mismo lugar que los demás mensajes de ubicación de almacenamiento.

Se puede producir un error de reparación en los siguientes casos:

- Formato `UserLayerRepair.json` incorrecto (poco probable, ya que se generan los archivos JSON).
- No se puede encontrar el archivo VHD o el archivo `package_app_rules` in-image de una capa de aplicación especificada.
- Error al adjuntar el archivo VHD de una capa de aplicación.

- Excepciones inesperadas (aleatorias) que interrumpen el proceso de reparación.

Si se produce alguno de estos problemas, el archivo UserLayerRepair.json NO se elimina y el procesamiento de los archivos JSON restantes se detiene.

Para identificar las razones exactas del error, revise el archivo ulayersvc.log del usuario. A continuación, puede permitir que la reparación se ejecute de nuevo en los inicios de sesión posteriores. Suponiendo que se resuelva la causa del error, la reparación finalmente se realizará correctamente y se eliminarán los archivos UserLayerRepair.json.

## Actualizar capa

December 4, 2023

Los pasos para actualizar el software en un sistema operativo, plataforma o capa de aplicación son prácticamente los mismos. Agregue una versión a la capa, instale la actualización o el parche en la máquina de empaquetado, verifique y, a continuación, finalice la capa. Una vez actualizada, implementa la nueva versión de capa, que varía según el tipo de capa.

La capa de plataforma es la capa de prioridad más alta y crítica para la implementación de imágenes, especialmente en lo que respecta a dispositivos, como las redes. Siempre que actualice el software de infraestructura, debe agregar una nueva versión a la capa de plataforma.

Agregue una versión a la capa de plataforma mediante la nueva capa del sistema operativo como base. Una vez que la máquina de empaquetado haya comenzado, apague la máquina para su finalización. La capa de plataforma reúne los componentes críticos de la nueva versión de capa del sistema operativo y los actualiza en la plataforma para que coincidan con la versión del sistema operativo.

## Agregar una versión a la capa

Por ejemplo, para agregar una versión a una capa de SO:

1. En la consola de administración de Citrix App Layering, seleccione **Capas > Capas** de sistema operativo
2. Seleccione una capa de SO y haga clic en **Agregar versión** en la ficha **Información de versión**.
3. En los detalles de la versión:
  - a) Para **Versión base**, seleccione la versión que se utilizará como base para la nueva versión de capa. El valor predeterminado es la última versión.
  - b) Introduzca un nombre para la **nueva versión**. Esta puede ser la versión del sistema operativo u otra información de identificación.



4. Seleccione una **configuración de Conector** para el hipervisor en el que cree la capa.
5. Introduzca un nombre de archivo para el disco de empaquetado y seleccione el formato de disco que se va a utilizar si utiliza el recurso compartido de archivos del dispositivo, en lugar de una configuración de conector. Este disco se utiliza para la máquina de empaquetado (la máquina virtual) donde se instala la aplicación.
6. Verifique la configuración y haga clic en **Agregar versión**. Esto ejecuta una tarea para crear una versión del sistema operativo. Cuando la tarea se completa, se muestra el estado **Acción necesaria**. Al seleccionar la tarea y hacer clic en **Ver detalles**, aparece el siguiente texto:

“Se ha publicado el disco de empaquetado. La máquina virtual ‘<...>’ se encuentra en la carpeta ‘<...>’ del centro de datos ‘<...>’. Encienda esta máquina virtual para instalar la aplicación. Cuando se complete la instalación, apague la máquina virtual antes de hacer clic en **Finalizar** en la barra de acciones.”

A continuación, puede implementar una máquina de empaquetado para esta versión de capa de SO.

### Implementar una máquina de empaquetado en el hipervisor

La máquina de empaquetado es una máquina virtual en la que se instalan las actualizaciones o aplicaciones que se incluirán en la capa. La máquina de empaquetado es una máquina virtual temporal que se elimina una vez finalizada la capa del sistema operativo.

La descripción de la tarea contiene instrucciones para desplazarse hasta la ubicación del hipervisor en la que se ha creado la máquina de empaquetado para esta capa.

1. Para crear la máquina de empaquetado en el hipervisor, comience con la tarea de disco de empaquetado expandido que se muestra en el paso 2.
2. Inicie sesión en su cliente de Hypervisor.
3. En la consola de administración, utilice las instrucciones de la tarea de disco de empaquetado expandido para desplazarse a la máquina de empaquetado.

### Instalar la actualización del sistema operativo

1. Inicie sesión remota en la máquina de empaquetado. Asegúrese de iniciar sesión en la cuenta de usuario que utilizó para crear el sistema operativo.
2. Instale las actualizaciones o aplicaciones que quiera incluir en la nueva versión de la capa del sistema operativo, como las actualizaciones de Windows o las aplicaciones antivirus.
3. Si la instalación de una aplicación requiere un reinicio del sistema, reinicie manualmente. La máquina de embalaje no se reinicia automáticamente.
4. Asegúrese de que la máquina de empaquetado está en el estado que quiere que sea para el usuario:

- a) Si las aplicaciones que instala requieren cualquier configuración posterior a la instalación o registro de aplicaciones, siga estos pasos ahora.
- b) Elimine los ajustes, las configuraciones, los archivos, las unidades asignadas o las aplicaciones que no desee incluir en la máquina de empaquetado.

A continuación, apague la máquina de empaquetado y verifique que la capa esté lista para finalizar.

**Nota:**

Al actualizar Windows 10 de una versión principal a otra (1703 a 1709, por ejemplo), la instalación anterior de Windows se deja en la carpeta C:\Windows.old. En App Layering, no debes eliminar esta carpeta. Nuestro software necesita copiar nuestros controladores y otros archivos de Windows.old a Windows una vez que la actualización haya finalizado por completo. Limpiaremos Windows.old cuando finalice la capa del sistema operativo.

### Verifique la capa y apague la máquina de empaquetado

El siguiente paso es verificar que la capa está lista para ser finalizada. Para estar listo para la finalización, se debe completar cualquier proceso posterior a la instalación, por ejemplo, un reinicio o un proceso `ngen` de Microsoft.

Para verificar que los procesos pendientes se hayan completado, puede ejecutar la herramienta Apagar para finalizar (icono a continuación), que aparece en el escritorio de la máquina de empaquetado.

Para utilizar la herramienta Apagar para finalizar:

1. Si no ha iniciado sesión en la máquina de empaquetado, inicie sesión remota como el usuario que creó la máquina.
2. Haga doble clic en el icono Apagar para finalizar. Una ventana de línea de comandos muestra mensajes que detallan el proceso de verificación de capas.
3. Si hay una operación pendiente que debe completarse antes de que se pueda finalizar la capa, se le pedirá que la complete. Por ejemplo, si una operación `ngen` de Microsoft debe completarse, puede intentar acelerar la operación `ngen`, como se detalla a continuación.
4. Una vez completadas las operaciones pendientes, vuelva a hacer doble clic en el icono Apagar para finalizar. Esto apaga la máquina de empaquetado.

La capa está lista para finalizar.

Si la configuración del conector que ha seleccionado está establecida en **Descarga de composición**, la capa se finaliza automáticamente. De lo contrario, el siguiente paso es finalizar la capa manualmente, como se describe en el siguiente procedimiento.

## Mensajes de integridad de capa

Los siguientes mensajes de integridad de capa le indican qué operaciones en cola deben completarse antes de que la capa esté lista para finalizar:

- A RunOnce script is outstanding - please check and reboot the Packaging Machine.
- A post-installation reboot is pending - please check and reboot the packaging machine.
- A Microsoft ngen operation is in progress in the background. - An MSI install operation is in progress - please check the packaging machine.
- A reboot is pending to update drivers on the boot disk - please check and reboot the packaging machine.
- A Microsoft ngen operation is needed.
- 'Software Center Client está configurado para ejecutarse, pero el archivo SMSCFG.INI sigue presente. Para obtener más información sobre la implementación de SCCM en un entorno virtual, consulte el artículo de Microsoft TechNet, [Implementación de SCCM en un entorno VDI de Xen-Desktop.](#)'

Para obtener más información sobre el significado de los mensajes de integridad de capa y cómo depurarlos, consulte [Depuración de problemas de integridad de capas en Citrix App Layering 4.x y versiones posteriores.](#)

No puede omitir los mensajes de integridad de capa apagando el equipo. El software App Layering se detiene y le devuelve a la máquina de empaquetado hasta que los procesos se hayan completado.

Si hay una operación `ngen` de Microsoft en curso, es posible que pueda acelerarla, como se describe en la siguiente sección.

## Agilizar las operaciones `Ngen.exe` de Microsoft, si es necesario

Una vez instaladas todas las actualizaciones de software, debe permitir a `Ngen.exe` básicamente recompilar código de bytes `.NET` en imágenes nativas y construir las entradas del registro para administrarlas.

`Ngen.exe` es el generador de imágenes nativas de Microsoft, que forma parte del sistema `.NET`. Windows determina cuándo se ejecuta `Ngen.exe` en función del software que se está instalando y de lo que detecta Windows en la configuración.

### Importante:

Cuando `Ngen.exe` se está ejecutando, debes dejar que se complete. Una operación `Ngen.`

`ngen.exe` interrumpida puede ocasionar que los ensamblados `.NET` no funcionen o que haya otros problemas en el sistema `.NET`.

Normalmente, `Ngen.exe` es una operación en segundo plano que se detiene cuando hay actividad en primer plano. Si quieres acelerar una operación `Ngen.exe`, puede poner la tarea en primer plano para completarla lo antes posible.

Para poner la tarea en primer plano:

1. Abra un símbolo del sistema como Administrador.
2. Vaya al directorio `Microsoft.NET\Framework` de la versión actualmente en uso:

```
cd C:\Windows\Microsoft.NET\FrameworkNN\vX.X.XXXXX <!--NeedCopy
-->
```

3. **Si utiliza .NET Framework 3 o posterior**, introduzca este comando de `Ngen.exe` para ejecutar todos los elementos en cola. Este comando procesa las instalaciones de componentes en cola antes de crear ensamblajes.

```
ngen eqi 3 <!--NeedCopy-->
```

La tarea `Ngen.exe` pasa al primer plano en la solicitud de comando y muestra los ensamblajes que se están compilando. Está bien si ve mensajes de compilación.

Asegúrese de que todos los procesos `Ngen.exe` se han ejecutado hasta su finalización. Puede utilizar el **Administrador de tareas** para ver si `MSCORSVW.EXE` se está ejecutando una instancia de. Si es así, permite que se complete o se ejecute `ngen eqi 3`.

#### Precaución:

No reinicie para detener la tarea. ¡Permita que la tarea se complete!

4. **Si utiliza .NET Framework 2 o anterior**, introduzca este comando de `Ngen.exe` para ejecutar los elementos en cola.

```
““ ngen update /force
```

```
1 Esto coloca la tarea ngen en primer plano en el símbolo del
 sistema y enumera los ensamblados que se compilan.
2
3 >***Nota:**
4 >No pasa nada si ves mensajes de **error de compilación**.
5 >Busque en el Administrador de tareas si se está ejecutando una
 instancia de MSWORD.EXE. Si lo está, debe permitir que se
 complete o volver a ejecutar 'ngen update /force \'. No
 reinicie para detener la tarea. Permita que se complete.
6
7 Para comprobar el estado de una operación `Ngen.exe`, abra un sí
 mbolo del sistema como administrador y ejecute este comando:
 ``ngen queue status<!--NeedCopy-->
```

**Precaución:**

No reinicie para detener la tarea. ¡Permita que la tarea se complete!

5. Cuando se hayan completado todas las operaciones, apague la máquina virtual mediante el acceso directo **Shutdown For Finalize** disponible en el escritorio.

## Finalizar la capa manualmente

Una vez creada la máquina de empaquetado y todas las aplicaciones o actualizaciones instaladas, puede finalizar la capa.

Nota: Al finalizar una nueva versión de una capa de SO, el sistema elimina la máquina de empaquetado para no incurrir en más costes.

Cuando una capa está lista para finalizar:

1. Vuelva a la consola de administración.
2. En el módulo Capas, seleccione la capa.
3. Selecciona **Finalizar** en la barra de acciones.
4. Supervise la barra de tareas para comprobar que la acción se completa correctamente y que la capa se puede implementar.

## Exportar e importar capas

July 6, 2022

La función *Exportar e importar capas* le permite exportar capas desde su dispositivo de App Layering e importar las capas en un dispositivo instalado en otra ubicación de su entorno. Por ejemplo, puede utilizar esta función para mover capas de un dispositivo en un entorno local a un dispositivo en un entorno de nube. O bien, desde un entorno de prueba de concepto hasta la producción.

El dispositivo ejecuta un análisis en cada capa que importa para determinar su idoneidad para las capas elásticas. Los resultados del análisis se incluyen en los detalles de la capa.

### Antes de comenzar

Antes de exportar o importar capas, cumpla los siguientes requisitos y revise las consideraciones relacionadas.

## Requisitos

Para exportar e importar capas necesita lo siguiente:

- Dispositivo que contiene las capas que quiere exportar.
- Dispositivo al que quiere mover las capas.
- Un recurso compartido de archivos de red SMB configurado que es:
  - Accesible por ambos dispositivos.
  - Tiene suficiente espacio para todas las capas exportadas, además de los metadatos e iconos para las capas.
- Información requerida:
  - Ruta de acceso, nombre de usuario y contraseña del recurso compartido de archivos de red SMB al que quiere exportar las capas.
  - Nombre y contraseña de administrador para la consola de administración.

## Consideraciones

Tenga en cuenta los siguientes puntos al exportar e importar capas.

### **Si los nombres de archivo del recurso compartido de archivos incluyen caracteres especiales**

Como el recurso compartido de archivos no admite algunos caracteres especiales, los nombres de las capas con caracteres especiales se cambian temporalmente a guiones bajos (\_) en el recurso compartido de archivos. Se cambian todos los caracteres no admitidos.

Por ejemplo, una capa denominada “Notepad++” se convierte en “Notepad\_” cuando se exporta. Cuando las capas se importan en el nuevo dispositivo, se restaura el nombre original y aparece de nuevo como “Notepad++”.

**Ejecutar no más de una importación o exportación a la vez** Solo se debe ejecutar una importación o exportación a la vez.

**La capa de SO necesaria debe incluirse en la exportación de capas** Puede copiar las capas exportadas a otro recurso compartido de archivos para importarlas, pero asegúrese de mover el archivo de capa de SO requerido junto con los demás archivos de capa. El dispositivo importa primero la capa de SO, porque la capa de SO es necesaria para importar otras capas.

**Denominación de capas para exportación** Todas las capas se exportan al siguiente directorio en el recurso compartido de archivos:

`\*recurso compartido de archivos de red*\ Unidesk\ Capas exportadas\`

Los nombres de archivo exportados reflejan el nombre de capa, el nombre de versión de capa y los GUID de capa.

**Selección de capas** Al seleccionar capas, los iconos no solo indican qué capas están seleccionadas, sino que también indican si una carpeta contiene capas que ya se han exportado o importado, dependiendo de la operación en la que se realice.

Al exportar capas:

- Si un icono está parcialmente seleccionado, significa que la carpeta incluye algunas capas que no están seleccionadas.
- Si un icono está atenuado, significa que no se puede seleccionar la capa para la exportación, lo más probable es que la capa ya se haya exportado. Pase el cursor sobre la capa para ver un mensaje acerca de por qué no se puede seleccionar.

Al importar capas:

- Si un icono está parcialmente seleccionado, significa que la carpeta incluye algunas capas que no están seleccionadas.
- Si un icono está atenuado, significa que no se puede seleccionar la capa para la importación, lo más probable es que la capa ya se haya importado. Pase el cursor sobre la capa para ver un mensaje acerca de por qué no se puede seleccionar.

**Búsqueda de capas** El cuadro **Buscar** le permite buscar todas las capas y versiones que contienen el texto de búsqueda. Las búsquedas *no* distinguen mayúsculas de minúsculas

Recuerde que al seleccionar una carpeta, la interfaz de usuario solo selecciona el subconjunto de capas visibles. Cuando una carpeta que selecciona tiene un icono *parcialmente* seleccionado, significa que algunas de las capas seleccionadas ya se han exportado o importado. Puede ver esas capas, que normalmente están ocultas, seleccionando la casilla de verificación **Mostrar versiones que no se pueden seleccionar** sobre la lista.

**Velocidad de búsqueda afectada por el número de niveles de subdirectorio** Al exportar una capa, si sus subdirectorios tienen varios niveles de profundidad, nuestro software escanea todos los niveles debajo de ese directorio y, por lo tanto, tarda más en mostrar los directorios.

**Eliminación de capas exportadas** Puede eliminar una capa exportada de la base de datos solo cuando no esté incluida en una plantilla de imagen.

## Exportar capas

1. En la consola de administración de App Layering, seleccione **Capas > Exportar**.
2. Introduzca la ruta del recurso compartido de archivos a la que desea exportar las capas. El software de App Layering agrega la siguiente ruta a la Convención de nomenclatura universal (UNC) que especifique:  

```
\Unidesk\ Capas exportadas
```
3. Introduzca el **nombre de usuario** y **la contraseña** de un administrador que tenga acceso total al archivo.
4. Haga clic en **Connect**. Si es necesario, ajuste las credenciales hasta que la prueba se realice correctamente. No puede continuar hasta que haya una conexión con el recurso compartido de archivos.
5. Elija las capas que desea exportar:
  - a) En **Selección de versiones**, haga clic en **Modificar selección** para mostrar las carpetas de las versiones de las capas de SO, las capas de plataforma y las capas de aplicaciones.
  - b) Si ya ha exportado a la ubicación seleccionada, puede hacer clic en la casilla **Mostrar versiones que no se pueden seleccionar** para mostrar las capas previamente exportadas a esta ubicación.
  - c) Seleccione las capas y versiones que desee exportar y, a continuación, haga clic en **Guardar**.
6. Haga clic en **Confirmar y completar** para comprobar que el espacio disponible no supera el tamaño estimado del archivo. Cuando hay suficiente espacio, el botón **Exportar capas** pasa a estar disponible. Si lo desea, puede introducir un comentario. Se crea una tarea *Exportar capas* en la que puede realizar un seguimiento del progreso.
7. Si cancela la exportación antes de que la capa del sistema operativo se exporte por completo, asegúrese de volver a exportar *todas* las capas, incluida la capa del sistema operativo.
8. Si crea más capas después de la exportación inicial, ejecute otra exportación a la misma ubicación. Solo se exportan las capas nuevas.

### Advertencia

No intente modificar ni cambiar el nombre de ninguno de los archivos exportados.

## Importar capas

Al importar capas de un dispositivo a otro, si dos capas tienen el mismo nombre aunque el contenido de la capa sea diferente, la capa importada tiene un “1” que acompaña al nombre. Si se importan otras capas con el mismo nombre, el “1” se incrementa.



**Nota:**

Para importar una capa de aplicación o plataforma, la capa de SO debe existir en el dispositivo o importarse al mismo tiempo. Puede importar varias capas a la vez y la capa del sistema operativo siempre se procesa antes que cualquier capa dependiente.

1. Inicie sesión en la consola de administración de App Layering y seleccione **Capas > Importar**.

**Nota:**

Puede anular la selección de capas individuales en la carpeta, como se explica en el paso #4 a continuación.

2. Introduzca la ruta al recurso compartido de archivos donde exportó las capas. Lo siguiente se anexa a la dirección URL especificada.

**\*\*\ Unidesk\ Capas exportadas\\*\***

3. Introduzca el **nombre de usuario** y la **contraseña** de un administrador que tenga *acceso total* al recurso compartido de archivos.
4. Haga clic en **Connect**. Si es necesario, ajuste las credenciales hasta que la prueba se realice correctamente.

El sistema compara el contenido del dispositivo con el del recurso compartido de archivos seleccionado y se prepara para importar las capas que aún no se han importado.

5. Elija las capas que desea importar:
  - a) Haga clic en **Modificar selección** para expandir la capa de SO que incluye las capas que desea importar y seleccione una de las subcarpetas que desee importar. De esta forma, se seleccionan todas las capas y versiones disponibles para su importación en la carpeta.
  - b) Si desea ver las capas que ya se han importado desde esta ubicación, hágalas visibles haciendo clic en la casilla **Mostrar versiones que no se pueden seleccionar**.
  - c) Si una de las carpetas incluye capas que *no* desea importar, anule la selección de cada una de esas capas.
6. Compruebe las capas que desea importar y, a continuación, haga clic en **Confirmar y completar**.
  - Verifique las capas en cola para su importación. Solo se enumeran las capas que *aún no se han importado* del recurso compartido de archivos.
  - Compruebe que haya suficiente espacio en el almacenamiento local del dispositivo para las capas. El sistema no permite que la importación continúe hasta que haya espacio suficiente para las capas.

### Importante

Si cancela una importación de capa de SO, se cancelan todas las importaciones de capas que dependen de la capa de SO.

7. Cuando todos los ajustes sean válidos, haga clic en **Importar capas**. Se crea una tarea Importar en la que puede realizar un seguimiento del progreso.

Una vez importadas las capas, se ejecuta un “Análisis de ajuste elástico” en las capas, lo que le permite ver qué capas se pueden asignar de forma elástica.

## Excluir archivos de capas (función avanzada)

January 12, 2024

Puede excluir archivos y carpetas específicos de una capa compuesta para evitar que los archivos persistan en el escritorio del usuario. Por ejemplo, puede excluir de un inicio de sesión a otro los archivos y carpetas del software antivirus que no deben permanecer en un escritorio.

Las exclusiones que defina se aplican a una capa compuesta, una vez que forma parte de una imagen publicada. Esta función no se aplica en una máquina de empaquetado, solo en una imagen publicada en la que se hayan compuesto las capas. Esto significa que usted define las exclusiones al crear la capa, incluir la capa en la plantilla de imagen y, a continuación, publicar la imagen.

### Exclusiones predeterminadas

Las actualizaciones de la herramienta Gold Image mantienen una carpeta de archivos.txt para introducir y acumular exclusiones predeterminadas para el sistema de archivos de App Layer. Las capas del sistema operativo deben actualizarse con las versiones más recientes de la herramienta para garantizar que se haya establecido el conjunto correcto y completo de exclusiones.

La ubicación de estas exclusiones predeterminadas es `C:\Windows\Setup\Scripts\CitrixDefaultExclusions\`. Los clientes no necesitan hacer nada con esta carpeta ni con su contenido. Cualquier exclusión nueva se puede eliminar mediante una revisión de la capa del sistema operativo si causa problemas a un cliente.

#### Nota:

Las instalaciones futuras de la herramienta Gold Image sobrescribirán los cambios locales realizados por los clientes, por lo que se recomienda informar de los problemas relacionados con las exclusiones predeterminadas.

Esta función complementa el método de entrega de exclusiones de usuario y sigue el mismo formato, restricciones y uso que `c:\Program Files\Unidesk\Uniservice\UserExclusions\` los archivos.

Los dos nuevos archivos de exclusiones predeterminados son `FsLogixExclusions.txt` y `GroupPolicyHistoryExclusions.txt`.

## Limitación

Los archivos y carpetas excluidos de las capas elásticas no se procesan. Las exclusiones solo se pueden procesar cuando están presentes en la imagen.

## Especificar archivos y carpetas para excluir

En la carpeta `C:\Program Files\Unidesk\Uniservice\UserExclusions\`, cree uno o más archivos `.txt` que especifiquen las rutas que se van a excluir.

Todas las rutas válidas a los archivos y directorios se excluyen y, a continuación, se leen de la imagen. Todos los cambios en esos archivos y directorios en la capa de escritura ya no persisten.

Si uno de los archivos que crea contiene una ruta no válida, el procesamiento de ese archivo se detiene y pasa al siguiente `.txt` archivo de la carpeta `\UserExclusions`.

También puede usar un carácter `*` como comodín en un directorio para su exclusión. Por ejemplo `C:\Users\*\AppData\Local\Temp\`, donde `*` indica cualquier nombre de usuario. En este caso, cualquier nombre de usuario que coincida con el resto de la ruta se ajusta a la regla de exclusión, lo que permite al administrador omitir el directorio `\Temp` del usuario para todos los usuarios que usen esa imagen.

Para cada regla de exclusión, solo puede usar comodín en un directorio (usar uno `*`) en una sola ruta. No puedes excluir varios directorios con uno solo `*`. Por ejemplo, el uso de la regla `C:\Top\*\Bottom\` excluye los archivos de los directorios `C:\Top\First\Bottom\`, `C:\Top\Second\Bottom\`, etc. Sin embargo, los archivos del directorio no `C:\Top\First\Second\Bottom\` se excluyen, porque hay dos directorios entre `\Top\` y `\Bottom\` en lugar de uno.

No hay límite en cuanto al número de reglas de exclusión que puede establecer que contengan un comodín (`*`).

## Ejemplos

Excluir un archivo:

```
1 c:\test\test.txt
2 <!--NeedCopy-->
```

Excluir un directorio:

```
1 c:\test\
2 <!--NeedCopy-->
```

### Restricciones

Las siguientes restricciones se aplican a las exclusiones.

#### Nombre del directorio

- Comience la ruta con C:\
- Termine con una barra invertida (\)

**Exclusiones** Estos directorios de nivel superior no se pueden excluir:

- C:\
- Archivos C:\Program\
- C:\Program Archivos (x86)\
- C:\ProgramData\
- C:\Windows\
- C:\Users\

Los siguientes caracteres y expresiones no están permitidos en las exclusiones:

- Sin signos de interrogación (?)
- Sin expresiones regulares (sin %x%)
- Sin barra inclinada (/)
- Sin red (\\)
- Sin ruta a un directorio diferente (\..\)
- Sin comillas (“)
- Sin dos puntos (:) después de C:\

### Registro

Los mensajes de registro están disponibles en:

```
1 C:\Program Files\Unidesk\Uniservice\Log\Log0.txt
2 <!--NeedCopy-->
```

Mensajes escritos en el registro:

- Exclusión de usuarios agregada: incluye los detalles sobre el archivo o el directorio.

- No se pudo agregar la exclusión de usuarios: incluye detalles sobre las exclusiones no admitidas.

## Publicar

November 5, 2020

El servicio Citrix App Layering le permite publicar imágenes *en capas* como discos compatibles con su plataforma. Puede utilizar una imagen en capas para aprovisionar máquinas virtuales, como lo haría con cualquier otra imagen.

### Acerca de las imágenes en capas

Las imágenes en capas son imágenes de arranque compuestas desde una capa de SO, una capa de plataforma y cualquier número de capas de aplicaciones.

Publicar imágenes en capas desde una plantilla de imagen. La plantilla de imagen permite especificar las capas que se incluirán en las imágenes por capas. También puede especificar lo siguiente:

- La configuración del conector que se va a utilizar para acceder a una ubicación del entorno.
- Si quiere habilitar las capas elásticas para entregar aplicaciones a los usuarios cuando inician sesión.
- Si se habilitan las capas de usuarios, que conservan los datos y la configuración de la aplicación de los usuarios.

### Imágenes en capas para sistemas de Provisioning

La forma en que se especifican las capas que se van a incluir en una imagen en capas consiste en guardar la combinación de capas que quiere para un grupo determinado de usuarios en una plantilla de imagen. A continuación, utilice esta plantilla para publicar una imagen en capas en la plataforma elegida.

Cuando necesite actualizar la imagen en capas, simplemente modifique la plantilla de imagen para agregar o eliminar asignaciones de capa y publicar una nueva versión de la imagen.

## Crear o clonar una plantilla de imagen

May 9, 2024

Una plantilla de imagen almacena la lista de capas que se van a incluir en las imágenes por capas que se publican. Desde una única plantilla, puede publicar tantas imágenes en capas como necesite para aprovisionar sistemas en una ubicación determinada.

Una vez que cree una plantilla de imagen desde cero, puede clonar la plantilla para crear rápidamente un conjunto de plantillas que tengan la misma configuración.

Cuando actualice el software en una capa de aplicaciones o plataforma, actualice las plantillas de imagen para utilizar la nueva versión de capa. Para entregar la nueva versión de capa a los usuarios, puede volver a publicar las imágenes en capas y utilizar las imágenes actualizadas para aprovisionar sus sistemas.

### Requisitos

Para crear una plantilla de imagen, utilice

- Capa de sistema operativo
- Capa de plataforma (opcional)

#### Importante:

Si usa la capa de plataforma, debe tener la misma configuración de hardware que la capa de sistema operativo. Esta configuración se elige al implementar la máquina virtual para las capas de sistema operativo y de la plataforma.

- Capas de aplicaciones (opcional)
  - No es necesario incluir capas de aplicaciones al crear una plantilla de imagen.
  - Puede agregar capas de aplicación a una plantilla de imagen y, a continuación, volver a publicar las imágenes en capas en cualquier momento.

Puede crear una plantilla de imagen sin capas de aplicaciones. Esto es útil para probar la capa de SO antes de usarla para crear capas de aplicaciones.

### Crear una plantilla de imagen desde cero

Para crear una plantilla de imagen:

1. En la consola de administración de App Layering, seleccione el módulo **Imágenes** y, a continuación, haga clic en **Crear plantilla**.
2. Introduzca un **Nombre** para la plantilla y las notas en el campo **Descripción** (opcional), de modo que pueda identificar la plantilla al elegir una para publicar una imagen en capas.

3. Seleccione una de las **capas de sistema operativo disponibles**. Si hay más de una versión de capa, la versión más reciente se selecciona de forma predeterminada. Puede seleccionar una versión anterior en el menú desplegable.
4. (Opcional) Seleccione las **capas de aplicaciones > Modificar selección** que quiera incluir en las imágenes en capas que publique con esta plantilla.
5. (Opcional) Seleccione una capa de plataforma con las herramientas y la configuración de hardware para el objetivo de imagen requerido.
6. Elija una **configuración de conector** para la plataforma en la que va a crear esta capa. Si la configuración que necesita no aparece en la lista, debe crear la configuración del conector desde la página **Conectores**.
7. Modifique los siguientes campos, según sea necesario:
  - **Nombre del archivo del disco de imágenes en capas (rellenado automáticamente):** el nombre del disco de imágenes en capas se rellena automáticamente a partir del nombre de la plantilla.
  - **Disco de imágenes en capas desfragmentado:** cuando está habilitado, el disco de imágenes en capas se desfragmentará. Esta opción solo está disponible para conectores de composición de descarga.
  - **Tamaño de partición de imágenes en capas:** se recomienda el tamaño de disco predeterminado de 100 GB.
  - **Formato de disco de imagen en capas:** el formato de disco predeterminado es VHD, pero también puede seleccionar VMDK o QCOW2. Si va a publicar en el recurso compartido de archivos del dispositivo en lugar de utilizar una configuración de conector, esta opción le permite elegir un formato de disco compatible con el entorno en el que está copiando el disco.
  - **Sysprep:** las opciones disponibles dependen del hipervisor o del Servicio de Aprovisionamiento especificados en la configuración del conector:
    - Azure, Hyper-V, XenServer, Nutanix, vSphere: el valor predeterminado es *Generalizado sin conexión*. (Para Azure, esta es la única opción).
    - Creación de máquinas, Citrix Provisioning, View: *No generalizado* es la única opción para la creación de máquinas, Citrix Provisioning y View que se ejecutan en cualquiera de los hipervisores.
    - Recurso compartido de archivos: el valor predeterminado es *No generalizado*, si se usa un recurso compartido de archivos en lugar de una configuración de conector.
  - **Capas elásticas:** seleccione la opción **Capas de aplicaciones** para activar las capas elásticas en esta imagen en capas.
  - **Capa de usuarios:** cuando está habilitada en la configuración del sistema, puede seleccionar la opción Capas de usuario **completas** (laboratorios), **Office 365** (escritorio) u **Office 365 de sesión** (sistema operativo de servidor). Elija la opción **Completo** para guardar

la configuración y los datos para los usuarios independientemente de las aplicaciones específicas. Elija **Office 365 u Office 365 de sesión** para guardar la configuración y los datos de Outlook 365 que se ejecuta en un sistema de escritorio o un host de sesión.

8. Seleccione **Confirmar y completare** introduzca los comentarios que desee para esta capa.
9. Haga clic en **Crear plantilla** para guardar los cambios o en **Crear plantilla y publicar** para guardar la plantilla y, a continuación, publicar las imágenes en capas.

El icono de nueva plantilla aparece en el módulo Imágenes.

## Clonar una plantilla de imagen

Puede crear una copia de una plantilla de imagen clonándola. Cada clon es una copia independiente del original. El historial de auditoría muestra que la plantilla se clonó “Creada (clonada)” e indica de qué imagen se clonó, “Clonada a partir de *nombre-plantilla*”.

El primer clon recibe el mismo nombre que la plantilla original, con “- Copy” anexo. A cada clon subsiguiente se le agrega “- CopyN”, donde *N* es un número de secuencia creciente. El número de secuencia se incrementa al primer número disponible, en lugar del número después del último que ya está en uso. El número máximo es 1000.

Para clonar una plantilla de imagen:

1. En la consola de administración de App Layering, seleccione el módulo **Imágenes**.
2. En el módulo Imágenes, seleccione una plantilla de imagen y haga clic en **Clonar** en la barra de acciones o en el menú emergente. Se crea una copia de la plantilla con “- Copy (1)” anexo al nombre.

Puede cambiar el nombre y modificar el clon para sus propósitos.

## Siguiente paso

Ahora puede usar la plantilla de imagen para [publicar imágenes en capas desde la plantilla de imagen](#)

## Publicar imágenes en capas desde una plantilla

May 9, 2024

Las imágenes en capas son máquinas virtuales compuestas a partir de las capas y configuraciones especificadas en una plantilla de imagen. Mediante una plantilla de imagen, puede publicar tantas



imágenes en capas como necesite en una ubicación de Provisioning Services o Hypervisor que especifique en la configuración del conector.

Cuando se publican imágenes en capas, puede utilizar scripts para realizar pasos importantes específicos de la capa. Por ejemplo, puede activar Microsoft Office, lo que puede ser necesario antes de que la máquina virtual se utilice como disco maestro para las herramientas de implementación.

El mecanismo utilizado para ejecutar estos scripts puede variar, incluida nuestra propia funcionalidad `kmssetup.cmd`, el soporte de ejecución única o incluso la ejecución manual de los scripts. Después de que se ejecuten todos los scripts u otros pasos manuales y la máquina virtual está en el estado pertinente, los scripts inician un apagado del SO invitado o manualmente. Si usa la funcionalidad `kmssetup.cmd`, hay un proceso documentado para iniciar un apagado después de que se hayan completado todos los scripts de capa y otras funciones `kmssetup`.

Para publicar una imagen en capas:

1. En el módulo Imágenes, seleccione una o varias plantillas de imagen que quiera publicar.
2. En el menú **Acción**, seleccione **Publicar imagen en capas**.
3. En la página **Confirmar y completar**, seleccione **Publicar imágenes en capas**. Para cada plantilla de imagen, se inicia una tarea denominada **Publicación de imágenes en capas**.
4. Compruebe la barra de tareas y, cuando se cree el disco para esta imagen, haga clic en el enlace de la descripción de la tarea para pasar a la siguiente etapa.

El enlace le lleva a una máquina virtual cuyo estado de creación depende de la plataforma en la que está publicando:

- **XenServer, MS Hyper-V, Nutanix (o servicio de aprovisionamiento en él):** la máquina virtual se crea, pero está desactivada. Inicie sesión como invitado y deje que la máquina ejecute los scripts especificados en la configuración del conector.
- **Azure (o Creación de máquinas para Azure):** una ventana para crear una máquina virtual está abierta, pero incompleta. Introduzca los valores requeridos, termine de crear la máquina y enciéndala. La máquina ejecuta todos los scripts especificados en la configuración del conector.
  - Un conector de Azure se usa específicamente para la creación de capas.
  - Un conector de creación de máquinas para Azure se usa específicamente para la publicación de plantillas.
- **Google Cloud:** crea una VM desde Google Cloud Image en la consola de Google Cloud y enciéndela como sistema operativo invitado.
- **VMware Cloud:** cree una VM con una plantilla de máquina virtual de VMware y enciéndala como sistema operativo invitado.

**Nota:**

Se requiere una **plantilla de máquina virtual de VMware**, en lugar de una plantilla de máquina virtual estándar, para que la red de la máquina virtual funcione correctamente.

5. Cuando la máquina virtual esté en el estado deseado, apáguelo. El estado de la tarea cambia a **Hecho**.
6. Utilice la información de la descripción de la tarea para desplazarse a la imagen del entorno.

### **Posible mensaje de error**

Si recibe el siguiente error y quiere iniciar sesión en la imagen publicada para realizar cambios, debe ser a través del usuario local y **no** de un usuario de dominio.

`This system was not shut down properly. Please log off immediately and contact your system administrator.`

## **Administrar una plantilla de imagen**

July 6, 2022

Siempre que cree una nueva capa o agregue una nueva versión a una existente, puede:

- Actualice las capas seleccionadas en sus plantillas de imagen.
- Utilice las plantillas para publicar nuevas versiones de las imágenes en capas.
- Utilice las nuevas imágenes en capas para aprovisionar manualmente los sistemas.

Puede cambiar o eliminar una plantilla sin afectar a las imágenes en capas publicadas anteriormente, porque una imagen *no* está asociada a la plantilla utilizada para crearla.

### **Actualizar plantillas de imagen con una nueva versión de capa**

Cuando agrega una nueva versión a una capa de aplicaciones o a una capa de SO, puede identificar rápidamente las plantillas de imagen que incluyen la capa y seleccionar las plantillas que quiere actualizar con la nueva versión.

1. En la consola de administración de App Layering, seleccione **Capasy**, a continuación, seleccione la subficha para el tipo de capa que va a actualizar.

2. Selecciona la capa que actualizaste y, a continuación, la nueva versión de la capa que deseas asignar.
3. Haga clic en **Actualizar asignaciones**. Se muestran las plantillas de imagen que incluyen esta capa.
4. Seleccione las plantillas de imagen a las que desee asignar la capa o la versión de la capa.
5. Haga clic en **Guardar**.
6. Haga clic en **Confirmar y completar**.

### Modificar cualquier configuración de plantilla de imagen

Cuando quiera cambiar la configuración que utiliza para publicar cualquiera de las imágenes en capas, puede modificar la plantilla de imagen que utilizó originalmente para publicar las imágenes en capas y publicar una nueva versión de las imágenes.

1. En la consola de administración de App Layering, seleccione **Imágenes**.
2. Seleccione la plantilla que quiera modificar y haga clic en **Modificar plantilla**.
3. Puede cambiar el **nombre**, la **descripción** y el **icono** de la imagen.
4. Seleccione una versión diferente de la capa de sistema operativo elegida expandiendo la capa y eligiendo una diferente.
5. Agregue o quite capas de aplicaciones para incluirlas en las imágenes en capas que publique con esta plantilla. Si hay más de una versión de una capa, puede elegir una versión diferente expandiendo la capa y eligiendo una diferente.
6. Cambie la ubicación en la que se publica la imagen en capas seleccionando una **configuración de conector** diferente.
7. Cambie la **capa de plataforma** seleccionada, si, por ejemplo, va a publicar en un entorno diferente.
8. Modifique los detalles del **disco de imágenes en capas**, por ejemplo, para habilitar la estratificación elástica en la imagen.
9. Haga clic en **Confirmar y completare** introduzca comentarios para esta capa.
10. Haga clic en **Guardar cambios de plantilla** o haga clic en **Guardar plantilla y publicar** para publicar las imágenes en capas después de guardar la plantilla.

### Eliminar una plantilla de imagen

Cuando ya no necesite una plantilla de imagen, puede eliminarla de la consola de administración.

Una plantilla de imagen no se puede eliminar mientras se utiliza para publicar imágenes en capas.

1. En la consola de administración, seleccione **Imágenes**.
2. Seleccione la plantilla que quiera eliminar y haga clic en **Eliminar plantilla**.
3. Escriba los comentarios que quiera y haga clic en **Eliminar plantilla**.

## Administrar

November 5, 2020

En esta sección se explica cómo administrar el servicio App Layering, incluidos:

- [Configuración del sistema](#)
- [Almacenamiento](#)
- [Configuración del dispositivo](#)
- [Servicios App Layering](#)
- [Usuarios](#)
- [Puertos de firewall](#)

## Configuración del sistema

May 9, 2024

Puede especificar la configuración de los siguientes parámetros de configuración del sistema haciendo clic en el botón **Editar** de cada opción, realizando los cambios y, a continuación, haciendo clic en el botón **Guardar**.

En esta sección se describe la configuración de cada dispositivo.

## Supervisión y almacenamiento

Los siguientes servicios se ejecutan en el dispositivo App Layering:

- Servicio de gestión
- Servicio de estratificación
- Servicio de servidor BITS

Para obtener más información, vaya a [Servicios de App Layering](#).

## Servicios de directorio

Puede configurar el dispositivo para que se conecte a un servicio de directorios, por ejemplo, Active Directory. Cuando te conectas a tu servicio de directorio, creas uno o más cruces de directorio para acceder a dominios u unidades organizativas específicos. El dispositivo no modifica el servicio de directorio al que se conecta. El software almacena en caché los atributos de cada entrada del servicio de

directorio para que, si la conexión con el servicio de directorio se pierde temporalmente, el software pueda usar la información almacenada en caché para las tareas de administración.

Para obtener más información, vaya a [Servicio de directorio](#).

### **Ubicaciones de almacenamiento de capa de usuarios**

El almacenamiento local del dispositivo es un repositorio de capas en el que el dispositivo crea, compone y almacena capas e imágenes en capas. Para comprobar la cantidad de espacio libre en el almacenamiento local del dispositivo, puede ver cuánto espacio en disco se utiliza en el módulo Sistema del dispositivo de administración.

Para obtener más información, ve a [Almacenamiento](#).

### **Recursos compartidos de archivos de red**

El recurso compartido de archivos de red se utiliza para:

- Empaquetar capas mediante el recurso compartido de archivos de red, en lugar de un conector para el hipervisor.
- Publique imágenes en capas en el recurso compartido de archivos de red, en lugar de utilizar un conector para su plataforma de publicación.
- Servir capas elásticas.
- Actualice el software App Layering.

### **Configurar recursos compartidos de archivos de red**

Para configurar el recurso compartido de archivos de red, especifique los valores siguientes:

- Ruta de acceso compartido de archivos SMB
- Nombre de usuario y contraseña

### **Probar recursos compartidos de archivos de red**

A continuación, pruebe la conexión al recurso compartido de archivos haciendo clic en **Probar recurso compartido de archivos SMB**. La prueba devuelve un mensaje que indica `Success` o `Failed to mount network file share path`. Puede introducir un comentario que describa los cambios.

## Configuración del certificado HTTP

Muestra el certificado de seguridad establecido actualmente. Utilice los botones **Cargar y Generar** para cargar un certificado existente o para generar uno nuevo. Si lo quiere, introduzca un comentario que describa los cambios realizados.

### Certificados de confianza

Cuando introduce la URL de la aplicación, se le redirige automáticamente a una conexión segura. Si especifica HTTPS como protocolo en la URL y la aplicación no incluye un certificado de seguridad de una entidad de certificación, se le pedirá que omita las advertencias de seguridad la primera vez que acceda a la aplicación.

Para eliminar la advertencia de seguridad, cargue un certificado de confianza que cree.

**Requisitos** Los requisitos para el certificado de confianza son:

- Debe ser un certificado de Privacy Enhanced Mail (PEM).
- Debe incluir tanto el certificado como la clave.
- No incluye una frase de contraseña.

**Crear una CSR** Debe generar un archivo CSR para entregárselo al proveedor de certificados para una solicitud de certificado. Como ELM se basa en CentOS Linux, se incluye OpenSSL. Utilice el [Asistente para CSR de OpenSSL](#) de DigiCert para generar el comando OpenSSL necesario. A continuación, puede usar Putty para iniciar sesión en la consola y pegar el comando **OpenSSL**, que genera la CSR. Consulte los comandos de **OpenSSL** en la [Guía de referencia rápida de OpenSSL](#).

### Carga del certificado

1. Cree el certificado PEM.
2. Inicie sesión en la utilidad App Layering CacheCloud Infrastructure Management.
3. Seleccione **Configuración > Cargar certificado SSL** en el panel de la izquierda.
4. Busque el archivo de certificado PEM autofirmado y haga clic en **Cargar**.
5. Reinicie el dispositivo de administración.

## Configuración de notificaciones

Puede configurar la configuración automática de notificaciones por correo electrónico para usted o para otros usuarios.

## Configurar notificaciones por correo electrónico desde el dispositivo

Para configurar las notificaciones por correo electrónico, complete los siguientes campos. Todos los campos son obligatorios.

1. En el campo Servidor de correo, escriba el nombre del servidor de correo electrónico o del servidor de retransmisión SMTP.
2. En el campo Puerto del servidor de correo, escriba el número del puerto que utiliza el servidor de correo electrónico para la comunicación.
3. En el campo Nombre de usuario, introduzca el nombre de usuario de la cuenta de correo electrónico que quiere utilizar para enviar notificaciones. Por ejemplo, [nombredeusuario@dominio.com](mailto:nombredeusuario@dominio.com).
4. En el campo Contraseña, introduzca la contraseña de la cuenta de correo electrónico.
5. En el campo De, escriba una dirección de correo electrónico para identificar el origen del mensaje de correo electrónico. Por ejemplo, si escribe [midirección@miempresa.com](mailto:midirección@miempresa.com), el mensaje de correo electrónico mostrará lo siguiente en el cuadro De de la notificación recibida:  
  
App Layering Manager [[midirección@miempresa.com](mailto:midirección@miempresa.com)]
6. En el cuadro Lista de destinatarios, introduzca las direcciones de correo electrónico que deben recibir las notificaciones. Utilice una coma o punto y coma para separar las direcciones de correo electrónico.
7. Haga clic en Probar configuración de correo electrónico para comprobar que la configuración del servidor de correo electrónico y la cuenta funcionan correctamente. Si la prueba se realiza correctamente, el software muestra un mensaje de éxito y envía a los destinatarios un correo electrónico de confirmación.
8. Escriba un comentario, si es necesario, y haga clic en **Guardar** para guardar la configuración del correo electrónico. Los comentarios que introduzca aparecerán en la vista Información Historial de auditoría.

## Configuración de seguridad y retención

- Especifique el número de minutos de inactividad antes de que la consola de administración cierre la sesión.
- Especifique el número de días que el dispositivo debe conservar las tareas completadas antes de eliminarlas.
- Especifique el número de días que el dispositivo debe conservar los archivos de registro de auditoría. Después de ese tiempo, el software comienza a sobrescribir el registro de auditoría.

- Especifique el espacio máximo en disco que se utilizará para todos los registros (en MB) y el número de días que deben conservarse los archivos de registro.
- Si lo quiere, introduzca un comentario que describa los cambios realizados.

### Información

En esta sección se muestra más información sobre Enterprise Layer Manager (ELM), como la **versión de ELM**, el hipervisor que se está utilizando y dónde ir para obtener soporte.

### Almacenamiento

November 5, 2020

El almacenamiento local del dispositivo es un *repositorio de capas* en el que el dispositivo crea, compone y almacena capas e imágenes en capas. Para comprobar la cantidad de espacio libre en el almacenamiento local del dispositivo, puede ver cuánto espacio en disco se utiliza en el módulo Sistema del dispositivo de administración.

1. Inicie sesión en la consola de administración y seleccione **Sistema > Administrar dispositivo**.
2. En la tabla Servicios, el Almacenamiento local para el servicio de capas muestra cuánto espacio se utiliza y cuánto es libre.

#### Nota

- El espacio en disco se muestra en Gigabytes basados en 1024, no en métricas.
- El espacio libre se actualiza cada vez que se completa un trabajo de servicio de capas. Si quiere asegurarse de que la página se ha actualizado, haga clic en el icono Actualizar situado justo encima de la subficha Administrar dispositivo.
- Al crear una capa o agregar una versión a ella, se necesita espacio adicional temporalmente para crear el disco de empaquetado. Puede calcular la cantidad de espacio necesario durante la creación de capas agregando los siguientes tamaños de capa:
  - El tamaño de la versión de la capa del sistema operativo que estás mediante.
  - El tamaño del disco grabable que quiere para la capa de aplicación.
  - El tamaño de cualquier capa de requisito previo (si tiene alguna).

### Agregar un disco al almacenamiento conectado localmente

Cuando instala el dispositivo, viene equipado con un disco de datos adicional de 300 GB que se utiliza como repositorio de capas. Puede expandir el almacenamiento local del dispositivo agregándole otro



disco.

Después de agregar un disco a la máquina virtual del dispositivo mediante la consola del hipervisor, siga estos pasos:

1. Inicie sesión en la consola de administración.
2. Seleccione **Sistema > Administrar dispositivo**.
3. Seleccione **Expandir almacenamiento**. Se muestra la ficha Selección de disco de discos que están conectados al sistema y que *no forman* parte del repositorio de capas.
4. Marque la casilla de verificación de cada disco que quiera utilizar para expandir el repositorio de capas. Si una casilla de verificación está atenuada y hay un icono amarillo con el símbolo ! (signo de exclamación), significa que el disco conectado no se puede utilizar (por ejemplo, si el disco no está vacío). Una vez que el disco conectado esté en blanco y sin particiones, podrá usarlo para expandir el almacenamiento local del dispositivo.
5. En la ficha Confirmar y completar, haga clic en **Expandir almacenamiento**.
6. Según las prácticas recomendadas, una vez que se haya agregado el disco, reinicie el dispositivo para que el disco se active.

### **Agregar espacio a un disco existente en el almacenamiento conectado localmente**

Si no es posible agregar un disco nuevo, puede agregar espacio a un disco de almacenamiento local existente de la siguiente manera.

1. Inicie sesión en la consola de administración del hipervisor y siga el procedimiento normal para aumentar el tamaño del disco de almacenamiento local (puede tener más de uno de estos discos y puede expandir cada uno de ellos).
2. Inicie sesión en la consola de administración y seleccione **Sistema > Administrar dispositivo**.
3. Seleccione Expandir almacenamiento. Se muestra una lista de discos expandidos (también puede ver discos adjuntos que aún no forman parte del repositorio de capas, pero puede ignorarlos).
4. Observe que el Nuevo tamaño del disco expandido es mayor que el Tamaño actual.
5. Marque la casilla de verificación del disco que quiere expandir hasta Nuevo tamaño.
6. En la ficha Confirmar y completar, haga clic en Expandir almacenamiento.

### **Agregar ubicaciones de almacenamiento para capas de usuarios**

Cuando habilita capas de usuarios en una imagen en capas, los datos y la configuración de cada usuario se conservan entre sesiones.

Al implementar con capas de usuarios habilitadas, puede agregar ubicaciones de almacenamiento para esas capas, en lugar de permitir que los datos del usuario se guarden en el recurso compartido de archivos principal del dispositivo.

Al configurar ubicaciones de almacenamiento de la capa de usuarios:

- Puede asignar grupos de usuarios a cada ubicación.
- La primera ubicación de almacenamiento agregada al dispositivo se convierte en la ubicación predeterminada para las capas de usuarios no asociadas a ninguna otra ubicación de almacenamiento.
- Las ubicaciones de almacenamiento se enumeran en orden de prioridad.
- Si un usuario pertenece a más de un grupo y esos grupos se asignan a diferentes ubicaciones de almacenamiento, la capa de usuarios de la persona se almacenará en la ubicación de almacenamiento de mayor prioridad. Una vez que la capa de usuarios de la persona se guarda en la ubicación de prioridad más alta, si cambia el orden de prioridad de las ubicaciones de almacenamiento a las que está asignado el usuario, los datos guardados hasta ese punto permanecerán en la ubicación de prioridad más alta anteriormente. Para conservar la capa de usuarios de la persona, *debe* copiar la capa de usuarios en la nueva ubicación de prioridad más alta.

### Crear ubicaciones de almacenamiento de capa de usuarios

Para agregar una ubicación de almacenamiento:

1. Inicie sesión en la consola de administración.
2. Seleccione **Sistema > Ubicaciones de almacenamiento de capa de usuarios**.
3. Seleccione **Agregar ubicación de almacenamiento**. Se muestra una lista de recursos compartidos de archivos, excepto el recurso compartido de archivos principal del dispositivo.
4. Seleccione **Agregar ubicación de almacenamiento** e introduzca un nombre y una ruta de red para la nueva ubicación.
5. En la ficha Asignaciones de capa de usuarios, expanda el árbol de directorios y marque las casillas de verificación de uno o más grupos para agregar a la nueva ubicación de almacenamiento.
6. En la ficha Confirmar y completar, haga clic en **Agregar ubicación de almacenamiento**.

A continuación, debe establecer la seguridad en las carpetas de capa de usuarios.

### Configurar la seguridad en las carpetas de capa de usuarios

Puede especificar más de una ubicación de almacenamiento para las capas de usuarios. Para cada ubicación de almacenamiento (incluida la ubicación predeterminada) debe crear una subcarpeta /Users y proteger esa ubicación.

El administrador de dominio debe establecer la seguridad de cada carpeta de capa de usuarios en los siguientes valores:

|                            |             |                                    |                                  |                                    |                                                                                                                                                                                                                               |                                                                                       |                                                                                                                                                  |                                                                                                                                                  |
|----------------------------|-------------|------------------------------------|----------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre de la configuración | Se aplica a | Propiedades de archivos y carpetas | Metadatos de archivos y carpetas | Ubicaciones de archivos y carpetas | Usuarios o grupos de carpetas                                                                                                                                                                                                 | Sistema de archivos                                                                   | Carpetas de administración                                                                                                                       | Carpetas de configuración                                                                                                                        |
|                            |             | so-<br>la-<br>mente                | so-<br>la-<br>mente              | o<br>car-<br>petas/<br>At-         | car-<br>car-<br>At-<br>jun-<br>se-<br>tar<br>lec-<br>ciosa-<br>nada<br>Recor-<br>rer<br>car-<br>peta/<br>E-<br>je-<br>cu-<br>tar<br>archivo,<br>Lis-<br>tar<br>car-<br>peta/<br>Leer<br>datos,<br>Leer<br>atrib-<br>u-<br>tos | to-<br>se-<br>tal<br>lec-<br>ciosa-<br>nada<br>sub-<br>car-<br>petas<br>y<br>archivos | de<br>to-<br>do-<br>tal<br>lec-<br>ciosa-<br>nada,<br>min-<br>ios<br>y<br>grupo<br>de<br>ad-<br>min-<br>is-<br>tración<br>se-<br>lec-<br>cionado | de<br>to-<br>do-<br>tal<br>lec-<br>ciosa-<br>nada,<br>min-<br>ios<br>y<br>grupo<br>de<br>ad-<br>min-<br>is-<br>tración<br>se-<br>lec-<br>cionado |

### Establecer seguridad en las carpetas de capa de usuarios

1. Inicie sesión en la consola de administración.
2. Seleccione **Sistema > Ubicaciones de almacenamiento de capa de usuarios**. Los recursos compartidos de archivos mostrados son las ubicaciones de almacenamiento definidas para las capas de usuarios. Por ejemplo, supongamos que ha definido tres ubicaciones de almacenamiento para poder administrar más fácilmente el almacenamiento para Grupo1 y Grupo2 por separado de todos los demás miembros de la organización:
  - Ubicación predeterminada: \MyDefaultShare\UserLayerFolder\
  - Grupo1: \MyGroup1\Share\UserLayerFolder\
  - Grupo2: \MyGroup2\Share\UserLayerFolder\ Nota: El recurso compartido de archivos principal del dispositivo, que se utiliza para almacenar capas de SO, aplicaciones y plataformas, no aparece como una ubicación de almacenamiento de la capa de usuarios.

1. Cree un subdirectorio \Users bajo cada recurso compartido de archivos:

- \MyDefaultShare\UserLayerFolder\Users\
- \MyGroup1Share\UserLayerFolder\Users\
- \MyGroup2Share\UserLayerFolder\Users\

1. Aplique la configuración de seguridad enumerada anteriormente a cada subdirectorio /Users.

## Configuración del dispositivo

November 5, 2020

El dispositivo Citrix App Layering es un dispositivo virtual que utiliza la tecnología Enterprise Layer Manager (ELM). El dispositivo coordina la comunicación y administra copias de las capas y las plantillas de imagen.

Basado en CentOS, el dispositivo aloja la consola de administración. La consola le permite crear y administrar capas. También le permite publicar imágenes en capas mediante esas capas.

Puede iniciar sesión en la utilidad Configuración del equipo para modificar la siguiente configuración de administrador:

- Contraseña
- Dirección de red
- Servidores NTP
- Zona horaria

### Nota

La configuración del dispositivo no se puede modificar en Azure.

## Antes de comenzar

Asegúrese de que:

- El dispositivo de App Layering se está ejecutando en el hipervisor.
- Tiene la contraseña de una cuenta con privilegios de administrador

## Inicie sesión en el dispositivo con una cuenta con privilegios de administrador

Con la consola del hipervisor o SSH, inicie sesión en el dispositivo como administrador. (La primera vez que inicie sesión, utilice la contraseña predeterminada, **Unidesk1**) Se abrirá la utilidad Configuración del equipo.

## Configurar redes (incluye la opción Dirección IP estática)

Puede cambiar la dirección IP y los servidores DNS del dispositivo. La **configuración predeterminada de DNS** se recupera mediante el Protocolo de configuración dinámica de host (DHCP).

Si DHCP no está disponible y selecciona **Estático**, se le pedirá que introduzca las direcciones **IP** de los servidores DNS.

### Nota:

Si cambia la dirección IP del dispositivo, debe registrar [manualmente el agente de App Layering con el dispositivo](#) para que el dispositivo pueda comunicarse con el agente.

Para cambiar la dirección IP del dispositivo:

1. Con la consola del hipervisor o SSH, inicie sesión en el dispositivo como administrador. (La primera vez que inicie sesión, utilice la contraseña predeterminada, **Unidesk1**) Se abrirá la utilidad Configuración del equipo.
2. En la solicitud de acción, escriba **C** (para Configurar red) y presione Retorno.
3. En el siguiente mensaje, escriba **D** para Dynamic (DHCP) o **S** para Static. Si elige **Estático**, se le pedirá la dirección IP y la máscara de subred. Introduzca también las direcciones predeterminadas para la puerta de enlace y el servidor DNS.
4. Cuando se le solicite, escriba **Y** para guardar la configuración.
5. En la solicitud de acción, escriba **Q** para salir.
6. Reinicie el dispositivo.

## Sincronizar el reloj del sistema con los servidores NTP

Puede sincronizar el reloj del sistema en el dispositivo configurando servidores NTP. Puede especificar:

- Cuántos servidores NTP necesita, siendo 6 el máximo.
- Agregar y quitar servidores NTP, según sea necesario.

Siempre que sea posible, los servidores existentes se utilizan como valores predeterminados.

1. Con la consola del hipervisor o SSH, inicie sesión en el dispositivo como administrador. (La primera vez que inicie sesión, utilice la contraseña predeterminada, **Unidesk1**) Se abrirá la utilidad Configuración del equipo.
2. En la solicitud de acción, escriba **N** para cambiar servidores NTP y presione Retorno. Aparecerá una lista de los servidores NTP actuales.
3. En el símbolo del sistema, especifique cuántos servidores NTP necesita escribiendo un número de 0 a 6. 0: Se quitan todos los servidores (recibirá una advertencia). 1—6: Se le pedirá que acepte o reemplace cada uno de los servidores actuales.

4. Para cada servidor, presione Entrar para aceptar el valor actual. O bien, introduzca una nueva dirección de servidor (Ejemplo: 3.pool.ntp.org). Una vez introducida la última dirección, se muestra un resumen del servidor NTP.
5. Escriba S para guardar la configuración.
6. En la solicitud de acción, escriba Q para salir.
7. Reinicie el dispositivo.

### Cambiar la zona horaria

1. Con la consola del hipervisor o SSH, inicie sesión en el dispositivo como administrador. (La primera vez que inicie sesión, utilice la contraseña predeterminada, **Unidesk1**) Se abrirá la utilidad Configuración del equipo.
2. En la solicitud de acción, escriba T para Cambio de zona horaria y presione Retorno. Se muestra la zona horaria actual.
3. Presione Entrar para mostrar las zonas horarias disponibles. Las zonas horarias enumeradas están en orden alfabético, comenzando por el
4. Avance a través de los códigos de zona horaria hasta que consulte los suyos: Enter: Avanza una línea a la vez. Re Pág Av Pág: Muestra la pantalla siguiente o anterior llena de opciones. O busque las zonas horarias: Escriba Barra (/) y parte del nombre que está buscando.
5. Cuando se muestre la zona horaria, presione Q para llegar al indicador.
6. Escriba el número de su zona horaria. Aparecerá la zona horaria introducida.
7. Presione Entrar para completar el cambio.
8. En la solicitud de acción, escriba Q para salir.
9. Reinicie el dispositivo.

## Servicios App Layering

November 5, 2020

Los siguientes servicios se ejecutan en el dispositivo App Layering:

- Servicio de gestión
- Servicio de estratificación
- Servicio de servidor BITS

Los servicios se muestran en la ficha Sistema.

## Servicio de gestión

El dispositivo de App Layering utiliza el servicio de administración para comunicarse con los siguientes servidores, agentes y software de plataforma:

- Active Directory
- Servidores de archivos de Windows
- Servidores de hora de red
- Servidores de archivos Unix
- Servidor DHCP
- Agentes App Layering
- Su Hypervisor y servicio de Provisioning

Los puertos de firewall para cada uno de los componentes anteriores deben estar abiertos. Para obtener más información, consulte [Puertos de firewall](#).

## Servicio de estratificación

El servicio de capas administra las capas y las plantillas de imagen. El dispositivo mantiene un conjunto de capas maestras en su almacenamiento local y capas elásticas en el recurso compartido de archivos del dispositivo.

**Nota: Las capas** elásticas son copias de capas de aplicaciones almacenadas en el recurso compartido de archivos del dispositivo. Las capas elásticas se entregan al iniciar sesión del usuario, en lugar de como parte de la imagen en capas.

En el módulo Sistema, el servicio de capas muestra la cantidad de espacio disponible en cada uno de los recursos compartidos de archivos.

## Servicio de servidor BITS

El dispositivo de App Layering copia archivos desde y hacia el dispositivo mediante el servicio Servidor BITS de Microsoft y la ubicación especificada en la configuración del conector.

### Puertos de firewall para el servicio Servidor BITS

Abra los puertos del firewall para el servicio Servidor BITS. Para obtener más información, consulte [Puertos de firewall](#).

## Registros del servidor BITS

BITS Server produce sus propios registros, que puede encontrar aquí:

`/var/log/Unidesk`

Los registros se basan en la configuración de log4net, que puede encontrar en la siguiente ubicación:

`source\BitsServer\Citrix.AppLayering.BitsServer\log4net.config`

## Si quiere cambiar la ubicación de la carpeta Subidas

Puede montar otro volumen para utilizarlo en las cargas de BITS configurando la ruta de acceso al volumen tanto para el servidor BITS como para el conector de Hyper-V.

1. Monte el nuevo volumen.
2. Modifique la ubicación de la carpeta Subidas para el servidor BITS en el siguiente archivo json:

`/var/aspnetcore/bits-server/appSettings.production.json`

Cambiar la configuración predeterminada de UploadFolder de `/mnt/repository/uploads` a la nueva ubicación, por ejemplo `/mnt/test/uploads`.

1. Busque el archivo de configuración del conector:

`/usr/local/lib/node_modules/unidesk-hyperv-connector/config.json`

Cambie la carpeta de carga predeterminada (llamada FileUploadFolderPath) de `/mnt/repository/uploads` a la nueva ubicación:

1. Reinicie ambos servicios:

```
1 systemctl restart kestrel-bits-server systemctl restart unidesk-hyperv-connector<!--NeedCopy-->
```

1. Actualice el grupo y los permisos en la nueva carpeta Cargas:

```
1 chmod 770 /mnt/test/Uploads chmod g+s /mnt/test/Uploads chgrp apache /mnt/test/Uploads<!--NeedCopy-->
```

## Servicio de directorios

July 6, 2022



Puede configurar el dispositivo para que se conecte a un servicio de directorios, por ejemplo, Active Directory. Cuando se conecte a su servicio de directorios, creará uno o más cruces de directorio para acceder a dominios o unidades organizativas específicos. El dispositivo *no* modifica el servicio de directorio al que se conecta. El software almacena en caché los atributos de cada entrada de servicio de directorios, de modo que si la conexión al servicio de directorios se pierde temporalmente, el software puede utilizar la información almacenada en caché para tareas de administración.

Al crear un cruce de directorios, utilice los siguientes acrónimos estándar del sector:

- OU: Unidad organizativa
- DC: Componente de dominio

### **Acerca de la conexión del dispositivo a un servicio de directorios**

En Management Console, System > Directory Services ( **Sistema > Servicios de directorio** ) muestra información sobre los usuarios y los grupos.

### **Protocolos compatibles**

Cuando se vincula a un servicio de directorios, el dispositivo de App Layering es compatible con los siguientes protocolos de capa de transporte y socket seguros:

- Capa de socket segura:
  - SSL 3.0
- Transport Layer Security:
  - TLS 1.1
  - TLS 1.2

### **Qué sucede cuando se agregan los cruces de directorio**

Cada cruce de directorios que cree especifica un nodo inicial en el árbol de directorios. Un nuevo cruce de directorio no puede incluir usuarios que ya sean miembros de otro cruce y los cruces no se pueden anidar.

Si agrega un cruce de directorio principal, todos sus secundarios se migran a ese cruce. Todos los usuarios y grupos importados se moverán al elemento principal, junto con todas las asignaciones elásticas. Después de mover, se eliminan los cruces de directorio secundario.

\*\*Si va a crear varios nombres distintivos

\*\*

El sistema compara primero el componente de dominio, las partes del nombre distintivo que comienzan con “**DC=**”. Tenga en cuenta que en Nombres Distinguidos, el pedido importa. Por ejemplo, **DC=A, DC=B** es diferente de **DC=B, DC=A**. El sistema agrega cruces de directorio independientes si sus componentes de DC difieren o si sus componentes de DC coinciden y los componentes restantes no se superponen. Los cruces de directorio se fusionan si sus componentes de DC coinciden y sus otros componentes están relacionados.

### Los atributos de usuario se importan desde el servicio de directorios

El software de App Layering importa y almacena en caché los atributos de usuario y grupo de su servicio de directorios cuando:

- Asignar privilegios de administrador a un usuario.
- Los valores de los atributos cambian en el servicio de directorios.

Los atributos que almacena en caché de software son de solo lectura. Todos los cambios en los atributos para los usuarios del servicio de directorios provienen del servidor de directorios.

### Los atributos importados se sincronizan regularmente

El software sincroniza la información que almacena en caché para los usuarios del servicio de directorios con el servicio de directorios cada 12 horas. Si el software descubre que un usuario ya no es un objeto en el servicio de directorios, clasifica al usuario como abandonado (puede ver esta información en la vista Información del usuario).

### Crear un cruce de directorio

1. Haga clic en **Sistema > Servicios de directorio**.
2. Haga clic en **Agregar cruce de directorios**.
3. Especifique los detalles del servidor de directorios:
  - **Dirección del servidor:** El nombre del servidor que utiliza para el servicio de directorio (dirección IP o nombre DNS).
  - **Puerto:** Especifique el número de puerto para comunicarse con el servidor de directorios.
  - **Usar SSL:** Haga clic para habilitar la comunicación de capa de sockets seguros (SSL). Si se producen errores de certificado, se muestra una lista de estos errores. Si está seguro de que es seguro ignorarlos, haga clic en **Aceptar y continuar**.
  - **Nombre distinguido (DN) de enlace:** Para determinar la sintaxis correcta para el nombre de usuario o el nombre de usuario de enlace, consulte la documentación de su directorio.

En los ejemplos siguientes se muestran algunas de las formas en que se puede especificar un usuario para el servicio de directorios:

- domain\username
- username@domain.com.
- **Contraseña** de enlace: escriba la contraseña.
- **Nombre distintivo base:** Especifique dónde comienza el software a buscar usuarios y grupos en el servicio de directorio remoto.
- **Nombre de cruce de directorios:** El nombre de la carpeta que se ve en la vista de árbol. Puede utilizar cualquier nombre, incluido el nombre de un dominio en el árbol de servicios de directorios.

4. Haga clic en **Confirmar y completar**.

## Usuarios

June 29, 2023

En esta sección se explica cómo [administrar sus usuarios y grupos de usuarios](#).

Para obtener más información sobre la asignación de funciones de usuario, consulte [Asignar roles](#).

Para obtener más información sobre cómo conectarse a un servicio de directorio, consulte [Conectarse a un servicio de directorio](#).

## Grupos y usuarios

June 29, 2023

Cuando instala por primera vez el dispositivo App Layering e inicia sesión en la consola de administración, hay una cuenta de administrador integrada que puede utilizar para empezar. Este administrador tiene derecho a realizar todas las operaciones de App Layering. Puede modificar las propiedades de este usuario, incluidos el nombre, la contraseña y la información de contacto. Asegúrese de cambiar la contraseña de esta cuenta de administrador integrada como parte de la instalación y configuración del dispositivo.

### Usuarios y grupos locales

La capa del sistema operativo conserva los usuarios o grupos locales que agregue, pero las capas de aplicaciones, las capas de plataforma, las capas de usuarios y las capas elásticas no lo hacen.

Por ejemplo, los usuarios y grupos que agrega o modifica al instalar una aplicación en una capa de aplicación, capa de plataforma o capa de usuarios no persisten. Agregue el usuario local o el administrador a la capa del sistema operativo antes de instalar la aplicación, o considere la posibilidad de instalar la aplicación en la capa del sistema operativo.

### Usuarios y grupos de AD

Además de la cuenta de administrador integrada, todos los usuarios y grupos son usuarios y grupos de AD importados a través de uno o varios cruces de directorios. Una vez creados los cruces de directorios, puede asignar funciones a cada usuario. Puede ver los roles asignados a un usuario en Detalles del usuario. Para obtener información detallada sobre la configuración, consulte [Conectarse a un servicio de directorio](#).

### Roles

Los roles determinan los módulos de App Layering que un usuario puede administrar. Al asignar roles a usuarios y grupos del Servicio de directorios, pueden usar sus credenciales del Servicio de directorios para iniciar sesión en la consola de administración. Para obtener más información sobre la asignación de funciones de usuario, consulte [Asignar roles](#).

### Puertos de firewall

May 9, 2024

El dispositivo de App Layering se comunica con el hipervisor, el servicio de aprovisionamiento y el agente App Layering. En este artículo se detallan los puertos que el dispositivo utiliza para comunicarse internamente con otros servicios relacionados con App Layering y externamente con servidores, como los servidores NTP. Asegúrese de abrir los puertos necesarios en el firewall antes de instalar el dispositivo de App Layering.

Durante la instalación de App Layering, abre los puertos que utiliza el dispositivo para interactuar con los servicios del servidor virtual en el que está alojado. Si hay un firewall entre el dispositivo de App Layering y el equipo en el que está ejecutando el agente App Layering o uno de los conectores de App Layering, debe abrir manualmente el puerto en el firewall utilizado para ese fin. Si durante la instalación ha cambiado alguno de los puertos de la configuración predeterminada, asegúrese de abrir el puerto correcto.

El dispositivo de App Layering utiliza el protocolo TCP/IP y se requiere IPv4. Hay tres clases principales de comunicación:

- Acceso y administración del dispositivo.
- Hablar con otro servicio de agente App Layering.
- Hablar directamente con hipervisores que no requieren el agente.

**Nota:**

El dispositivo de App Layering debe estar conectado a un recurso compartido de archivos de red.

### Usuario administrador

De forma predeterminada, App Layering usa los siguientes puertos del cortafuegos para que el usuario administrador interactúe con la consola de administración de la máquina virtual del dispositivo App Layering.

### dispositivo de App Layering

Los servicios de conector para los diversos hipervisores y servicios de aprovisionamiento enumerados a continuación se ejecutan en el dispositivo de App Layering.

| Destino de App Layering                       | Actividad                 | Protocolo | Puertos                   |
|-----------------------------------------------|---------------------------|-----------|---------------------------|
| Dispositivo                                   | Consola de administración | TCP       | 80, 443                   |
| Servicio de conector de Azure antiguo         | Comunicación              | TCP       | 3000 (HTTP), 3500 (HTTPS) |
| Servidor BITS                                 | Carga de disco            | TCP       | 3015 (HTTP), 3515 (HTTPS) |
| Servicio de conector de Citrix Provisioning   | Comunicación              | TCP       | 3009 (HTTP), 3509 (HTTPS) |
| Servicio de conector de Google - Google Cloud | Comunicación              | TCP       | 3016 (HTTP), 3516 (HTTPS) |
| Servicio de conector de Hyper-V               | Comunicación              | TCP       | 3012 (HTTP), 3512 (HTTPS) |

### Conexiones internas

De forma predeterminada, el servicio App Layering usa los siguientes puertos del cortafuegos para las conexiones internas entre el dispositivo y cada uno de sus destinos.

En la tabla, se usa la siguiente abreviatura:

- **Dispositivo** : el dispositivo virtual App Layering.
- **Agente** : se refiere al agente de App Layering.
- **Usuario administrador: usuario** de la consola de administración al que se le asigna la función de administrador de App Layering.
- **Máquina de composición: una máquina** virtual que se utiliza para crear y actualizar capas mediante el [motor de composición](#) de App Layering, que incluye:
  - Máquina virtual que se crea cuando se usa un conector con la **composición de descarga** habilitada para crear una capa, agregar una versión a una capa o publicar una imagen en capas.
  - Máquina virtual en la que se ejecuta el script `ImportOsLayer.ps1` para importar la imagen del sistema operativo como una nueva capa del sistema operativo.

| Origen de App Layering | Destino de App Layering | Actividad                                                | Protocolo | Puertos                   |
|------------------------|-------------------------|----------------------------------------------------------|-----------|---------------------------|
| Agente                 | Dispositivo             | Inscripción inicial                                      | TCP       | 443                       |
| Dispositivo            | Agente                  | Comunicación                                             | TCP       | 8016                      |
| Agente                 | Dispositivo             | Registrar las entregas del agente                        | TCP       | 8787                      |
| Dispositivo            | Hosts de vCenter, ESXI  | Comunicación con almacén de datos a través del host ESXI | TCP       | 443                       |
| Dispositivo            | Active Directory        | LDAP                                                     | TCP       | 389, 636                  |
| Dispositivo            | Máquina de composición  | Comunicación                                             | TCP       | 443                       |
| Máquina de composición | Dispositivo             | Comunicación                                             | TCP       | 443                       |
| Máquina de composición | Dispositivo             | Acceso al disco mediante iSCSI                           | TCP       | 3260                      |
| Usuario administrador  | Dispositivo             | Comunicación con conectores antiguos de Azure            | TCP       | 3000 (HTTP), 3500 (HTTPS) |
| Dispositivo            | Azure                   | Comunicación                                             | TCP       | 443                       |

## App Layering

---

| Origen de App Layering                       | Destino de App Layering | Actividad                                        | Protocolo | Puertos                   |
|----------------------------------------------|-------------------------|--------------------------------------------------|-----------|---------------------------|
| Usuario administrador                        | Dispositivo             | Comunicación del conector de Citrix Provisioning | TCP       | 3009 (HTTP), 3509 (HTTPS) |
| Agente en el servidor de Citrix Provisioning | Dispositivo             | Descarga de disco                                | TCP       | 3009 (HTTP), 3509 (HTTPS) |
| Usuario administrador                        | Dispositivo             | Comunicación del conector de Hyper-V             | TCP       | 3012 (HTTP), 3512 (HTTPS) |
| Agente en el servidor Hyper-V                | Dispositivo             | Descarga de disco                                | TCP       | 3012 (HTTP), 3512 (HTTPS) |
| Agente en el servidor Hyper-V                | Dispositivo             | Carga de disco                                   | TCP       | 3015 (HTTP), 3515 (HTTPS) |
| Dispositivo                                  | vSphere                 | Comunicación                                     | TCP       | 443                       |
| Dispositivo                                  | XenServer               | Comunicación                                     | TCP       | 5900                      |
| Dispositivo                                  | Prisma                  | Carga de disco                                   | TCP       | 2222                      |
| Dispositivo                                  | Prisma                  | Comunicación                                     | TCP       | 9440                      |

---

### Conexión externa

De forma predeterminada, usa el siguiente puerto del firewall para las conexiones externas entre el dispositivo App Layering y el destino que se indica a continuación.

**Nota:**

El dispositivo solo puede acceder a estas direcciones URL mediante las credenciales definidas para él. Si intenta navegar por estos sitios, aparecerá un mensaje de error.

## App Layering

---

| Destino de App Layering                                   | Actividad                            | Protocolo | Puertos |
|-----------------------------------------------------------|--------------------------------------|-----------|---------|
| <https://<br>applayeringwebapi<br>.azurewebsites.<br>net> | Acceso a API                         | TCP       | 443     |
| <http://alcdn.<br>citrix.com/>                            | Descargar medios de<br>actualización | TCP       | 80      |

---

### Imagen del sistema operativo, un requisito de XenServer

| Destino   | Actividad    | Protocolo | Puertos |
|-----------|--------------|-----------|---------|
| XenServer | Comunicación | TCP       | 5900    |

---

### Puertos clave

#### Administración y acceso básicos de los dispositivos (siempre necesario)

- HTTP: Puerto 80
- HTTPS: Puerto 443
- SSH: Puerto 22

### Servidores

- Servidor de Active Directory: Puerto 389: Protocolo LDAP
- Servidor de Active Directory: Puerto 636: Protocolo LDAPS
- Servidor de Active Directory: Puerto 53: Protocolo DNS
- Servidores de archivos Windows, SMB: Puerto 445: Protocolo SMB
- Servidores de tiempo de red: Puerto 123: Protocolo NTP
- Servidores de archivos Unix: Puerto 2049: Protocolo NFS
- Servidor DHCP, DHCP: Puerto 67: Protocolo UDP
- Dispositivo de App Layering: Puerto 68: Protocolo DHCP

### Agente de App Layering

El agente utiliza los siguientes puertos para las comunicaciones consigo mismo y con el dispositivo.



- Dispositivo a servidor agente:
  - Comandos del dispositivo/SOAP: Puerto 8016
- Servidor del agente al dispositivo:
  - Registro: Puerto 443 HTTPS
  - Exportación de troncos: Puerto 8787
  - Descarga de disco de Citrix Provisioning: Puertos 3009 HTTP, 3509 HTTPS
  - Descarga de disco Hyper-V: Puertos 3012 HTTP, 3512 HTTPS
  - Carga de disco Hyper-V: puertos 3015 HTTP, 3515 HTTPS

### **Conectores a hipervisores y servicios de Provisioning**

Los conectores del dispositivo permiten que el dispositivo se comunique directamente con los hipervisores compatibles y los servicios de aprovisionamiento mediante los siguientes puertos.

- XenServer: puerto 5900
- Citrix Provisioning: Puerto 8016 (agente de App Layering)
- Google Cloud: puerto 443
- Administración de Microsoft Azure: Puerto 443
- Microsoft Hyper-V: puerto 8016 (agente de App Layering)
- Nutanix AHV - Puerto 2222, 9440
- VMware vSphere: puerto 443 (hosts de Virtual Center y ESX para transferencias de discos)



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).